Agenda Item 7

7

SHEFFIELD CITY COUNCIL
Report to Council

Report of:	Deputy Chief Executive
Date:	13 June 2012
Subject:	Changes to the Constitution
Author of Report:	Dave Ross – Democratic Services 0114 273 5033

Summary:

This report provides details of proposed changes to the Constitution.

Recommendations:

That Council is recommended to approve the following changes to the Constitution, as set out in the appendices to the report:

(a) Part 4 – Amended Council Procedure Rule 13.1 (b)

(b) Part 4 – Revised Financial Procedure Rules (Financial Regulations)

(c) Part 5 – Revised Officers' Code of Conduct

Background Papers:

Revised Constitution February 2012.

Category of Report: OPEN

Statutory and Council Policy Checklist

Financial implications
NO
Legal implications
YES
Equality of Opportunity implications
NO
Tackling Health Inequalities implications
N/A
Human rights implications
N/A
Environmental and Sustainability implications
N/A
Economic impact
N/A
Community safety implications
N/A
Human resources implications
N/A
Property implications
N/A
Area(s) affected
None
Relevant Scrutiny Committee if decision called in
Not applicable
Is the item a matter which is reserved for approval by the City Council?
Yes
Press release
NO

1. Introduction

1.1 This report provides details of proposed changes to the Council's Constitution.

2. Background

2.1 To ensure that the Constitution is kept up to date, there is a regular review process every six months and, where changes are required, these are submitted to Full Council for approval. Changes were last approved by Full Council in February 2011.

2.2 In addition, the Director of Legal Services, in consultation with the Lord Mayor, has delegated authority to make any minor and consequential drafting changes to the Constitution.

3. Proposed Changes and Reasons

3.1 A minor change is proposed to Council Procedure Rule 13.1 (b) relating to petitions required a Council debate. There have also been revisions to the Financial Procedure Rules (Financial Regulations) and the Officers' Code of Conduct. Consultation on these changes has taken place with the Corporate Members' Governance Group.

Part 4 – Council Procedure Rule 13

3.2 Procedure Rule 13.1 (b) relates to petitions requiring a Council debate and is being amended to reflect current practice. The proposed change is set out at Appendix 1.

Part 4 - Financial Procedure Rules (Financial Regulations)

3.3 The Financial Regulations are an important part of the Council's financial governance arrangements. They provide the rules for the Council to follow so as to protect public money and give clarity for both Members and Officers regarding responsibilities for financial management.

3.4 The Regulations have been revised to ensure consistency with the Constitution and Leader's Scheme of Delegation, the Financial Protocols and Financial Polices have been updated and there have been a number of presentational changes. A summary of the proposed changes and a revised version of the Financial Regulations are attached at Appendix 2.

Part 5 – Officers' Code of Conduct

3.5 The Code has been updated and includes revised Council policies, ensures consistency with the Member/Officer Protocol and takes account of legislation, such the Equality Act 2010. A summary of the proposed changes and a revised version of the Code are attached at Appendix 3.

4. Legal Implications

4.1 Except where delegated by Council (see paragraph 2.2 above), variations to the Constitution may only be made by Full Council.

5. **Recommendations**

5.1 That Council is recommended to approve the following changes to the Constitution, as set out in the appendices to the report:-

(a) Part 4 – Amended Council Procedure Rule 13.1 (b)

(b) Part 4 – Revised Financial Procedure Rules (Financial Regulations)

(c) Part 5 – Revised Officers' Code of Conduct

Lee Adams, Deputy Chief Executive

13 Petitions

13.1 The Council has adopted a Petitions Scheme which can be found on the Council's website (www.sheffield.gov.uk/petitions) and is one way in which citizens can express their concerns and priorities to the Council. Petitions can be presented to a meeting of the Council, Cabinet, Overview and Scrutiny Committee or Community Assembly and fall into three main types:-

(a) Ordinary Petitions

Comprising at least five signatures from members of the public requesting some form of action. As a courtesy, Democratic Services should be notified of the intention to present a petition at the earliest opportunity and no later than 10.00 a.m. on the day of the meeting in respect of Full Council meetings. The Council, on a Motion which need not be in writing and which shall be put without discussion, may (i) refer the petition to the appropriate body or appropriate Cabinet Portfolio holder for consideration or (ii) decide that no further action be taken on the matter.

(b) Petitions requiring a Council Debate

A petition containing 5,000 signatures or more will trigger a public debate by Full Council. Seven working days notice submitted to the Head of Democratic Services should be given to ensure Members have adequate preparation time. ~~A time limit of 40 minutes will be available for public debate to include three minutes for the lead petitioner to address the Council on the subject of the petition and subsequently within the overall time frame to answer any questions from Members. If the subject matter is within the Council's remit, Council can decide to take the action the petition requests, or not to take the action requested for reasons put forward in the debate. If the matter is one that falls under the remit of the Executive, Full Council can decide whether or not to submit recommendations as to how the final decision should be made. The Council can commission further investigation into the matter, for example by a relevant Committee, individual Cabinet Member or Executive Director.~~

The debate will be conducted and concluded as follows:-

- A 40 minute time limit for the item, with Members able to speak for up to three minutes each.

Formatted: Indent: Left: 3.81 cm, Tabs: Not at 1.27 cm

Formatted: Bullets and Numbering

- The petition representative will be given 3 minutes to present the petition at the beginning of the debate at the meeting.

Formatted: Indent: Left: 3.81 cm, Tabs: Not at 1.27 cm

Formatted: Bullets and Numbering

- The Lord Mayor will facilitate discussion of the petition by Members. Members' contributions will be summarised within the minutes of the meeting in order for the reasons for any subsequent referral to another body to be captured and communicated along with the petition, or for the reasons for the Council subsequently deciding to take no action on the petition to be recorded.

Formatted: Indent: Left: 3.81 cm, Tabs: Not at 1.27 cm

Formatted: Bullets and Numbering

- At the conclusion of the debate, the Lord Mayor will offer a "right of reply" to the representative of the petitioners so that he/she can respond to any matters raised in the debate. With the consent of the Lord Mayor, the representative may nominate another representative, who is entitled to speak under the Constitution, to provide that reply.

Formatted: Indent: Left: 3.81 cm, Tabs: Not at 1.27 cm

Formatted: Bullets and Numbering

- The Lord Mayor will outline the options/courses of action available to the Council based on the nature of the petition and invite Members to propose simple motions in accordance with the relevant options/courses of action available to the Council. He/she may also put forward his/her own suggestion in the light of the debate, or if no other motion is proposed by Members, or in order to facilitate a consensual course of action in the event that multiple, similar motions are proposed. Any motion proposed will need to be seconded. Motions will be either to:-

Formatted: Indent: Left: 3.81 cm, Tabs: Not at 1.27 cm

Formatted: Bullets and Numbering

    - note and take no action for the reasons put forward in the debate, or
    - take the action requested by the petitioners (if its within the Council's remit to do so), or
    - refer the petition to either the Cabinet, a Scrutiny Committee, a Cabinet Member or an Executive Director for consideration having regard to the

Formatted: Bullets and Numbering

comments made by Members during the course of the debate.

- If only one motion has been proposed and seconded, the Lord Mayor will call for a vote on that motion, which will either be carried or lost.

Formatted: Indent: Left: 3.81 cm, Tabs: Not at 1.27 cm

Formatted: Bullets and Numbering

- Should multiple motions have been proposed and seconded, the Lord Mayor will outline each motion and then call for a vote on each motion in turn until a motion is carried and an outcome is achieved.

Formatted: Indent: Left: 3.6 cm, Hanging: 0.85 cm, Tabs: Not at 1.27 cm

Formatted: Bullets and Numbering

(c) Petitions requesting evidence from an Officer.

A petition containing 2,500 signatures may ask that a Senior Officer gives evidence at a public meeting of one of the Council's Overview and Scrutiny Committees about something for which the Officer is responsible as part of their job.

13.2 Members of the public shall have an opportunity to address the Council or relevant Committee in respect of their petition for which they are the lead petitioner for a maximum of three minutes within the allocated time under Council Procedure Rule 15.1 for Public Question Time and Petitions, with the exception of petitions requiring a public debate under Council Procedure Rule 13.1(b) in which a total of 40 minutes will be available for the debate, inclusive of the three minutes for the lead petitioner to present the petition.

14 Communications

Each meeting of the Council will include an item of business to receive any communications or announcements that the Lord Mayor, the Leader of the Council or the Chief Executive may wish to place before the Council.

15 Public Question Time and Petitions

15.1 At Council Meetings

(a) A period of up to one hour shall be allocated at each ordinary meeting of the Council for the presentation of ordinary petitions and for written or oral questions submitted by members of the public on matters relating to the City of Sheffield or the services provided by the Council to be answered by the Leader of the Council or the appropriate Cabinet Member. Employees of the

APPENDIX 2

Financial Regulations 2012

Brief summary of changes

Annual update	Main changes
• To ensure consistency with Constitution and Leaders Scheme	Definitions of Virements and Variations amended to be in line with Constitution. Budget Carry Forwards and Transfers to Specific Reserves added.
• To reflect changes in systems / practice etc	'60 day rule' for debts paid after this time Changes consequent on the move to e-Business, Requirement to comply with the Council's Document and Records Management Policy.
Financial Protocol	Main changes
• Changes to reflect new structure at FLT level • Framework of Financial Accountability	Updated list of authorised signatories for grant claims and banking transactions Amended to stipulate that EDs and DoBs **will** develop a Framework of Financial Accountability and it will link to the signing of the Protocol Reference to details of the Business Unit hierarchy in each Portfolio etc being attached to the Regs have been removed. Up to date Portfolio templates now available for signature
Financial Policies	Main changes
• Regulations to be 'one-source of the truth' for financial management principles	Principles in the existing (out of date) Policies reviewed and amalgamated into the Regulations as appropriate. Document Retention Schedule now Appendix C of the Regulations
Presentational	Main changes
	Income Management section – covers setting fees and charges through to write-off of debt. Reflects priority given to income generation and collection. Consistent arrangement of responsibilities at start of each Chapter, i.e. Members (if applicable), Exec Directors, Director of Finance, others as appropriate.

Sheffield City Council

Financial Regulations

2012

Version Control table

VERSION:	**Version 1.00**
DATE OF ISSUE:	**XX. XX. 2012**
AUTHOR:	**Larraine Manley / Eugene Walker**
APPROVED BY:	**Approved by Council XX.XX.2012**
STATUS:	**Approved Version**

Drafting process

Version Number	Date	Author	Reason for change
0.01 – 0.09(a)	01.02.2012 to 28.05.2012	Ann Rodgers and various reviewers	For full details see V0.09(a)

Table of Contents

Key Terms and Definitions

Annual Revenue Budget	This is the Council's total Revenue spending plans for the year including the level of Council Tax for the coming year. It is set by Council following receipt of the Annual Budget Report.
Asset(s)	The CIPFA Code of Practice on Local Authority Accounting in the UK 2010/11 defines an asset as 'a resource controlled by the authority as a result of past events and from which future economic benefits or service potential is expected to flow to the authority'.
Budget carry forward	A budget carry forward is an underspend of a specified amount of budget which is planned for, and transferred to an earmarked reserve to be spent in a future year(s) for a specified purpose. For the purposes of these Regulations this is treated as a Virement (See below)
Capital Programme	This is the sum of all the Council's individual capital projects and sub-programmes that the Council is planning to undertake during the ***coming 5 years***, together with the funding that will support the Programme. The Capital Programme is made up of a number of different projects ranging from large scale projects such as Building Schools for the Future to smaller projects such as children's play equipment. The number and size of the projects may change which means that Capital Programmes may not be comparable in terms of size and scope over time.
Capital Project	A project which uses capital resources to acquire assets, and /or build, improve, increase the market value of, or substantially lengthen the useful life of an asset.
Capital Reporting and Approval Timetable	This sets out the deadlines for submission of Capital Approval Forms, dates of review meetings, monitoring and forecasting cycles, reporting dates and finance system schedules.
Capital Spending	Spending to purchase, build, improve, increase the market value of or substantially lengthen the useful life of an asset. Examples include the Decent Homes Programme, Building Schools for the Future and the Local Transport Plan.
Corporate Plan	The Corporate Plan sets out the vision for the Council and Sheffield. It includes what the Council will do over the next three years in order to deliver the vision.
Director	An Officer who is a member of the Council's Director's Group.
The Executive	The Executive means the Leader of the Council and the Members selected by him / her to form the Cabinet. In line with arrangements made by the Leader's Scheme, the members of the Executive, individually and / or collectively, discharge the Council's executive functions, either themselves or though further lawful delegations of authority.

Back to Contents page

Executive Director	For the purposes of these Regulations, the term Executive Directors means the officers described in Part 7 of the Council's Constitution.
External Funding	As defined by the Chartered Institute of Public Finance and Accountancy, External Funding is "discretionary money not accounted for within the Formula Spending Share (the normal funding from central government) or equivalent, distributed by various UK and EU agencies on a business case and / or competitive basis requiring an application".
Finance Business Partners	Members of the Finance Service with specific responsibility for supporting Executive Directors and their teams through the provision of financial advice and decision support.
Finance Service	The Council's consolidated financial support service led by the Director of Finance.
Financial Policies	The Council has a detailed set of financial policies which underpin these regulations.
Financial Protocol	The Financial Protocol summarises the relationship between Executive Directors and the Director of Finance and is signed annually by all parties.
Forward Capital Programme	This is the term used to describe the projects that are intended (planned) to be in the Council's Capital programme for the following financial year. Information is usually prepared and collated in the autumn / winter for presentation to Council in March.
Inclusion	This is the term used for the incorporation of approved capital projects in the Forward Capital Programme **and** the addition of projects to the Forward Capital Programme at any time in the financial year, e.g. where a stream of funding is identified in December that needs to be spent before the end of March.
Leader	The Leader of the Council or, if the Council's executive arrangements are changed to a mayoral model, the Mayor (but not the Lord Mayor) of the Council.

Back to Contents page

Leader's Scheme	The scheme of delegation and / or other arrangements for exercising the Council's executive functions made from time to time pursuant to Section 14, Local Government Act 2000 by the Leader.
Medium Term Financial Strategy	The Council's Medium Term Financial Strategy presents an overview of the Council's Financial position over at least the next three year period including revenue and capital spending plans linked to priorities.
Portfolio	The name given to a group of departments managed by an Executive Director. The Executive Directors combine to make up the Council's Chief Officer Board (Executive Management Team).
Revenue Spending	Any expenditure by the Council that falls outside the definition of Capital Spending. Typically the day- to- day running costs of the Council such as salaries, rent, utility bills and payments to service providers.
Section 151 Officer	Under Section 151 of the Local Government Act 1972 and s114 of the Local Government Finance Act 1988, the Chief Finance Officer has a statutory responsibility to ensure that the Council makes arrangements for the proper administration of its financial affairs. The Executive Director – Resources is the responsible officer (Chief Finance Officer) for the purposes of s151.
Senior member of the Finance Service	These are the officers designated in para A3.5 of the Financial Protocol appended to these Regulations.
Sundry Debt	Miscellaneous income that is due to the Council that can be collected by payment up front or by raising a sundry debt invoice. Local taxation, housing benefit overpayments and rental income are not included in this definition.
Transfer to a specific reserve	A transfer to a specific reserve is funding that is being put to one side as part of the service's budget strategy. The funding will be used in future years for reinvestment back into the service area. For the purposes of these Regulations this is treated as a Virement (See below)
Utilities / Utility Bill	As approved by the Director of Commercial Services, payments for the following services are considered to be Utilities. Gas, Electricity, Water, Telecomms, Mail Services and Photocopiers.
Variation / Change in Scope (Capital)	This is where there are changes in the agreed capital project cost or outputs. This could be an increase in the cost of the project, a change in available funding, or what will be delivered (the outputs). For example, funding to refurbish six schools is reduced such that only three can now be delivered. This would create a financial variation and change of scope which require approval by Cabinet.
Variations (Revenue)	Variations are changes to the total amount of expenditure across either a Portfolio, Service or the Council as a whole **that result** in a change to the Council's **overall level of resources** as set out in the Budget **and approved by Council**

Back to Contents page

Virement	Virement is defined by CIPFA as the transfer of underspending on one budget head to finance additional spending on another budget head. Virements are also used to move budgets where a function is moved from one Portfolio or Service to another.
Write -Off	Removing a debt from the Council’s accounts using money that has been set aside as part of the bad and doubtful debt provision. It relates to debts that are correctly due to the Council but for whatever reason are no longer collectable.

Back to Contents page

Background

1.1. The purpose and authority of the Financial Regulations

These Regulations form part of the Council's Constitution and as such carry with them the same authority. They set out the financial management policies of Sheffield City Council and are the key part of the Council's financial governance arrangements.

They are intended to help Members and Officers manage the Council's finances in line with best practice and should be read and implemented in the wider context of the Council's decision making framework including the Constitution and the Leader's Scheme.

As per Section 2.2.7 of these Regulations, the Director of Finance is required to formulate and maintain any standards, procedures and processes as she / he deems necessary to support the effective implementation of these Regulations.

It is important that these Regulations are, and continue to be, relevant to the Council. They are regularly reviewed so as to be consistent with the Council's Constitution, Leader's Scheme of Delegation and all other related documentation. They are also reviewed in line with accounting best practice, legislation, and changing service needs.

Amendments cannot be made to these Regulations without the express consent of the Director of Finance.

Officers should initially contact their Finance Business Partner if they wish to raise any issues with the content of these Regulations.

1.2. Accountability for compliance

All officers are accountable for following the rules set out in these Regulations and it is important that Managers at all levels in the Council ensure that they, and their staff, are familiar with these Regulations and the rules they contain.

The Directors of Business Strategy are responsible, within their Portfolios, for ensuring compliance with these Regulations

These Regulations are a key element of the Council's governance arrangements. All Directors are required to sign the Annual Governance Statement (AGS) to confirm that they fully comply with the prescribed governance arrangements of the Council including these Regulations.

Non-compliance with these Regulations may result in the withdrawal of delegated financial authority and / or the application of disciplinary procedures.

Adherence to the processes associated with the Council's finance system (Oracle Enterprise One and QTier) is also essential to ensuring that officers are complying with these Regulations.

Back to Contents page

1.3. Accounting Policies

The Director of Finance is responsible for selecting Accounting Policies and ensuring that they are applied consistently. The Accounting Policies are set out in the Statement of Accounts which is prepared as at 31st March each year. The key controls in Accounting Policies are that;

- Systems of internal control are in place to ensure that financial transactions are lawful,
- Proper accounting records are maintained
- Financial statements are prepared which present fairly the financial position of the authority and its expenditure and income

1.4. Risk management

These Financial Regulations and associated finance systems and processes are a key part of the Council's risk management framework and associated risk strategies. By following these Regulations, the Council's finance processes, and ensuring that the financial risks and opportunities of any activity are fully considered and recorded in line with the risk management framework Officers will demonstrate compliance with corporate risk management requirements.

1.5. Internal Control

Internal Control is the system put in place by the Council to conduct its business in an orderly and efficient manner. It is used to safeguard its assets and resources, to deter and detect errors, fraud and theft, to ensure accuracy and completeness of its accounting data, to produce reliable and timely financial and management information and ensure adherence to the Councils policies and plans.

As part of the Annual Governance process, Directors and Executive Directors must confirm that they have satisfactory arrangements in place to manage internal controls within their Portfolio. This includes the requirement for individual managers to be responsible for the effectiveness of the internal control system within their Service.

Directors and Executive Directors are also required to highlight deficiencies in the control framework and to identify significant incidents that have occurred.

An Annual Governance Statement is prepared and signed by the Council's Section 151 Officer, Chief Executive and Council Leader. The statement describes the Council's governance framework and highlights any significant deficiencies.

The Audit Committee (or any future committee that may be given this function) is responsible for approving the Annual Governance Statement which is published along with the Council's Annual Accounts.

Back to Contents page

1.6. Training and development

The Director of Finance and the Executive Directors are jointly responsible for working co-operatively to ensure the effective implementation of these Regulations and management of the Council's financial arrangements. This will involve a commitment to influencing the culture of financial management through training and development of Portfolio managers and Finance Service staff to meet the required financial competencies.

The Director of Finance is responsible for producing documentation that supports these Regulations. These documents set out in more detail the Council's procedures and processes for carrying out work related to financial management and administration.

The Director of Finance is responsible for ensuring that appropriate training is made available to support these Regulations and associated procedures and processes.

Officers at all levels, and particularly managers, have a key role in recognising and identifying any training requirements they have to comply with these Regulations.

Finance Business Partners will work with Officers and Members to ensure that any training and competency requirements are identified and delivered.

Executive Directors are responsible for ensuring that the training opportunities which have been made available are taken up by their staff as required.

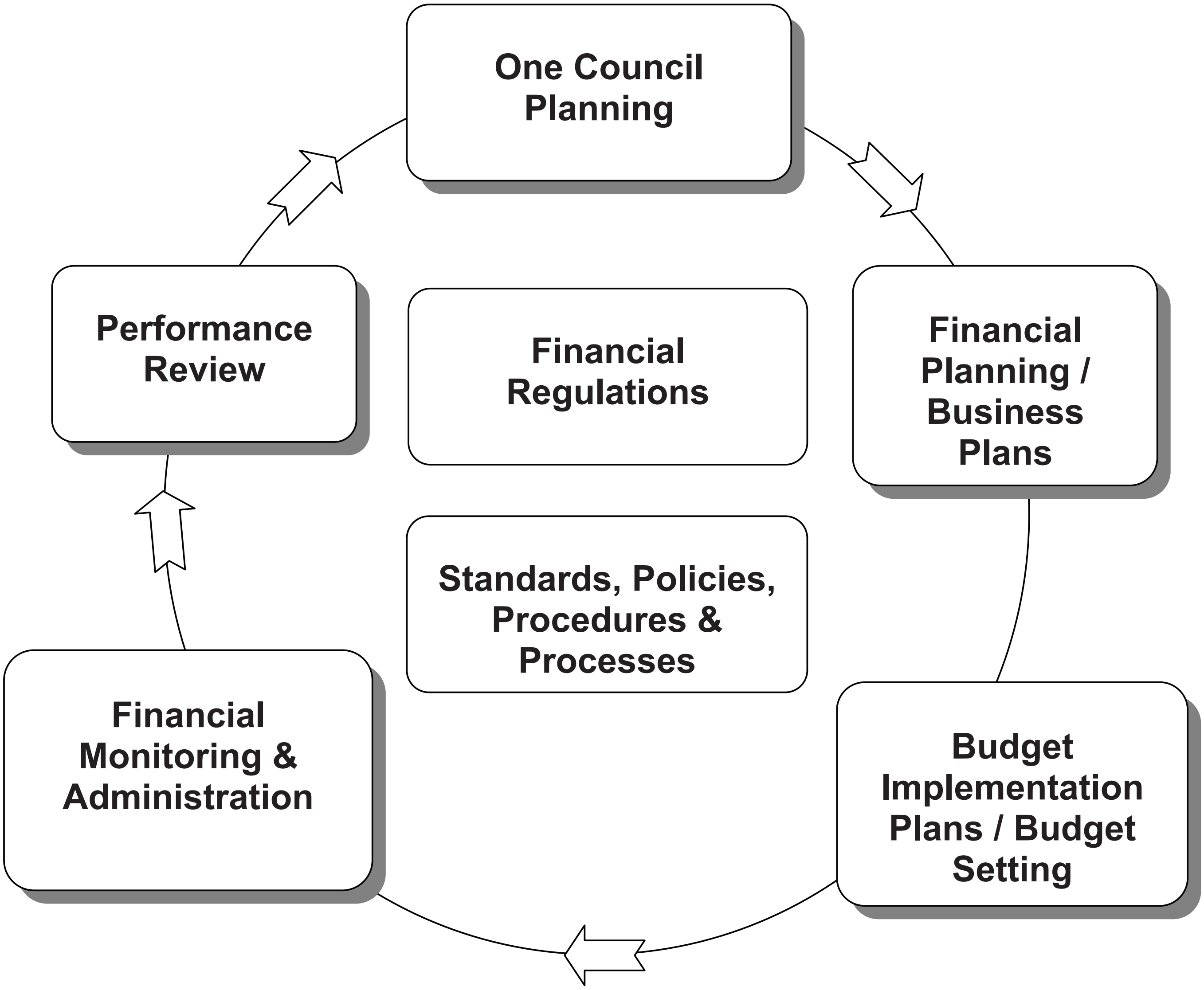
The training and guidance provided as part of the Council's finance system (Oracle Enterprise One and QTier) are in line with these Regulations.

Back to Contents page

2. Financial Management

2.1. The Cycle

The following diagram illustrates the financial management process starting with service planning and ending with the review of performance before the cycle starts again. These Financial Regulations and the financial policies and procedures issued by the Director of Finance are shown as supporting the financial management process.


One Council Planning
Financial Planning / Business Plans
Budget Implementation Plans / Budget Setting
Financial Monitoring & Administration
Performance Review
Financial Regulations
Standards, Policies, Procedures & Processes

Back to Contents page

2.2. Responsibilities and Delegated Authority

Many of the Council's responsibilities for finances are delegated within a framework of powers from Full Council to its committees (e.g. Audit Committee, Community Assemblies) and Officers, or from the Leader, primarily through his / her Scheme of Delegation of Executive Functions (e.g. to Cabinet, Individual Cabinet Members, Community Assemblies and Officers). Scrutiny Boards also have a role in the Council's financial management process.

2.2.1. Full Council

Functions reserved to Full Council include setting the Council's Annual Revenue Budget, the Housing Revenue Account, the overall Capital Programme and Council Tax levels, and approving or adopting the Policy Framework.

Functions exercised by Full Council are set out in Article 4 of the Council's Constitution.

If the Cabinet, individual Members of the Cabinet and any officers, Community Assemblies or joint arrangements which discharge executive functions have any doubt whether a proposed decision is in accordance with the approved Corporate Plan, Revenue Budget or Capital Programme, they must take advice from the Monitoring Officer and the Director of Finance.

If the advice of either of those officers is that a decision would not be in line with the approved Corporate Plan, Annual Revenue Budget or Capital Programme, then, subject to the rules of virement, (See S3.5) and subject to the urgency procedure the decision may only be taken by the Council.

2.2.2. The Executive

The Executive has overall responsibility for ensuring that the Council's expenditure remains within the resources available to it.

The Leader decides which parts of the Executive may exercise which executive functions and will generally do this through the Leader's Scheme.

If any lawfully made provision of the Leader's Scheme contradicts any provision of these Regulations, the Leader's Scheme shall prevail.

2.2.2.1. Cabinet

The Cabinet will receive a monthly budget monitoring report outlining the financial position for the whole Council.

The Cabinet will receive the out-turn report following the end of the financial year to approve decisions on the carry-forward / carry-back of resources from one year to the next.

The Cabinet may receive financial information during the year if an in-year decision on the Council's budget is required.

Back to Contents page

2.2.2.2. Individual Cabinet Members

Functions which may be exercised by individual Cabinet Members are set out in the Leader's Scheme.

All Cabinet Members will receive monthly budget monitoring reports for their areas of responsibility, via the relevant Finance Business Partner.

2.2.3. Community Assemblies (Area Committees)

Each Community Assembly has executive powers to approve expenditure of any amounts delegated to it by the Executive. Community Assemblies cannot spend money other than that allocated by Council or the Executive. Whenever a Community Assembly spends money, it must comply with these Regulations, Standing Orders, Commissioning and Procurement Guidelines and any other relevant policies or procedures.

Functions exercised by Community Assemblies are set out in;

- Article 10 of the Council's Constitution
- the Leader's Scheme
- Part 3 of the Council's Constitution

2.2.4. Audit Committee

The Audit Committee of the Council forms a key part of the governance of the Council. The terms of reference for the Audit Committee are set out in the Council's Constitution. The main financial duties are;

- To approve the Council's Statement of Accounts (which includes the Annual Governance Statement) in accordance with the Accounts and Audit Regulations 2003 as amended.
- To consider the Annual Letter from the Auditor or the Audit Commission in accordance with the Accounts and Audit Regulations 2003 as amended and to monitor the Council's response to any issues of concern identified.
- Monitoring the work of the Council's Internal Audit function

2.2.5. Strategic Resources and Performance Overview and Scrutiny Committee

The Strategic Resources and Performance Overview and Scrutiny Committee (or any future committee that may replace it) may request monthly budget monitoring reports. The reports will provide Members with overview financial information and report progress against the Annual Revenue Budget and Capital Programme budget set by Full Council. They will be provided by the Director of Finance in line with the budget reporting timetable.

The terms of reference for the Committee and its functions are set out in Article 6 and Part 3 of the Council's Constitution.

Back to Contents page

Scrutiny Committees can make recommendations to the decision makers but they do not make resource allocation decisions and therefore cannot approve changes in the budget or financial actions such as transfers to or from reserves. Decisions such as this can only be taken by Full Council or in accordance with the Leader’s Scheme or as otherwise directed by the Leader (section 14 Local Government Act 2000).

In relation to financial management and planning, the Strategic Resources and Performance Overview and Scrutiny Committee (or any future committee that may be given this function) is responsible for exercising an overview and scrutiny function in respect of:

- all the Council's strategic and longer term planning and corporate development issues;
- the budget setting process and budget monitoring;
- financial processes and day-to-day management of all the Council's internal resources, including finance, staffing and property.

Where a scrutiny board considers that a decision of the Executive is, or would be, contrary to, or not wholly in accordance with, the Council’s Corporate Plan, Annual Revenue Budget or Capital Programme, then it will seek advice from the Monitoring Officer and either the Executive Director of Resources or the Director of Finance.

2.2.6. Executive Directors

Each Executive Director will be responsible for ensuring the proper financial management of their Portfolio services and compliance with these Regulations by staff within their Portfolio.

Executive Directors are responsible for ensuring that a clear, written accountability framework is in place for the budgets held by each Service and Budget Manager.

Executive Directors will make appropriate arrangements for the discharging of their financial responsibilities by Directors and Managers within their Services. These arrangements must be fully compliant with the Council's financial policies and standards. They will not diminish the ultimate financial responsibilities of Executive Directors.

2.2.7. Executive Director of Resources and the Director of Finance

The Executive Director of Resources is the responsible officer (Chief Financial Officer - CFO) for the purposes of s151 of the Local Government Act 1972 and s114/114A of the Local Government Finance Act 1988. The Executive Director of Resources therefore has a statutory responsibility to ensure that the Council makes arrangements for the proper administration of the Council’s financial affairs. This includes ensuring the production and monitoring of these Regulations.

Back to Contents page

The Executive Director of Resources, as a member of the Council's Executive Management Team will ensure that the s151 role is discharged at this strategic level. On a day-to-day basis all s151 responsibilities may be discharged by the Director of Finance, who will act on behalf of the Executive Director of Resources in ensuring proper discharge of these statutory responsibilities. Nothing in this paragraph diminishes the ultimate financial responsibilities of the Executive Director of Resources. Whenever these Regulations provide that something will, must or may be done by the Director of Finance, this may also be done instead by the Section 151 Officer.

The Director of Finance is authorised to sign any and all grant claims, statutory returns or other documents that require the authority of the s151 officer on behalf of the Council.

The Director of Finance will be responsible for recommending amendments to these Regulations to the Council where she / he considers these to be in line with any changes to recommended best practice or essential service requirements or as otherwise appropriate. Minor and consequential amendments may be made by the Director of Legal Services in consultation with the Lord Mayor.

The Director of Finance will be responsible for fully documenting financial standards, policies, procedures, forms, etc which support these Financial Regulations by setting out in more detail the Council's procedures for carrying out finance work.

The Director of Finance is also responsible for ensuring that appropriate training is made available to support these procedures. Executive Directors are responsible for ensuring that these training opportunities are taken up by their staff.

The respective roles and responsibilities of Executive Directors and the Director of Finance in financial management are specified in a Financial Protocol document which will be signed annually by the Director of Corporate Resources, each Executive Director and their respective Director of Business Strategy.

2.3. Asset Management

The Executive is responsible for the Council's Asset Management Strategy and ensuring that the Council has an up-to-date Asset Register. Such responsibility is to be discharged in accordance with the Leader's Scheme.

2.3.1. Director of Finance

The Director of Finance has overall responsibility for the financial elements of Council's Asset Register and for ensuring that it complies with all necessary accounting requirements.

The Director of Finance is responsible for approving the use of leases to finance purchases. Revenue costs will be met from within Portfolio cash allocations, agreed as part of the Annual Revenue Budget process.

Back to Contents page

2.3.2. Director of Property & Facilities Management

The Director of Property & Facilities Management is responsible for Asset Management across the Council.

2.3.3. Executive Directors and the Director of Property & Facilities Management

Executive Directors and the Director of Property & Facilities Management are responsible for ensuring adequate arrangements are in place for maintaining and safeguarding the Council's property assets used for their Portfolios. When market conditions are favourable this includes consideration of the disposal of surplus capital assets as part of the Council's Asset Management Plan.

2.3.4. Disposal of surplus Capital Assets

Disposal of surplus assets must be done in accordance with the requirements of the Leader's Scheme.

2.4. Financial Risk Management

Specific responsibilities relating to risk management are set out in the Risk Management Framework and Guidance that was produced and agreed by Corporate Risk Management Group (CRMG).

Executive Directors are responsible for ensuring that risk management and business continuity are embedded at all levels within their area of responsibility in line with the Risk Management Framework and, in respect of financial risk management, ensuring the effective stewardship of public funds.

Financial Risk Management is built into these Regulations and many of the core processes that the Council expects managers to follow on a day-to-day basis. The Council's Risk Management strategy is based on good risk management being an integral part of good management and not a separate activity. Key mainstream processes that promote good risk management include, but are not limited to:

- Budget Monitoring
- The financial Administration processes in these Regulations
- The Council's Decision Making processes
- Programme and Project Risk Management
- Key Financial Risk Registers

In line with the requirements of the Risk Management Framework, Directors are responsible for maintaining and monitoring a Service Risks and Assurances log which must include financial risks.

Executive Directors are responsible for identifying and controlling risks in their area and significant financial risks should be reported to the Directors of Business Strategy.

The Director of Finance will report the most significant of these risks to the Council's Executive Management Team on a monthly basis and key risks will be summarised and reported to Members in monthly budget monitoring reports.

Back to Contents page

2.4.1. Money Laundering

Specific responsibilities relating to money laundering are set out in the Anti-Money Laundering Policy. This was produced by Internal Audit on behalf of the Director of Finance.

In line with the Anti-Money Laundering Policy, the Director of Finance is the Officer nominated to receive disclosures about Money Laundering activity within the Council – the MLRO.

The roles and responsibilities of the MLRO are set out in Appendix B to the Policy.

Executive Directors are responsible for ensuring that this policy is adhered to.

2.4.2. Fraud

Officer responsibilities in relation to fraud and corruption are set out in Appendix B of the Council's Code of Conduct: Policy Statement on Fraud and Corruption as set out in the Council's Constitution.

In accordance with Section 16 of these Regulations, Executive Directors are responsible for notifying the section 151 officer where there is any actual or suspected irregularity affecting the Council's assets.

2.5. Insurance

2.5.1. Executive Directors

Executive Directors are responsible for ensuring that prompt notification is given to the Director of Transformation Services and Performance of all circumstances involving both existing and new risk, the occurrence of which could result in the Council incurring a substantial liability. This will include details about Members, Officers, service users, third parties, property, vehicles, plant/ other assets, trading activities undertaken with organisations external to the Council, and any alterations affecting existing insurances, as well as potential insurance claims that may result from acts or omissions on the part of the Council.

They are responsible for ensuring that the insurance cover chargeable to their Portfolio budgets is accurate and up to date.

Executive Directors must immediately notify the Insurance & Risk Team of any loss, liability or damage or any event likely to lead to a claim and take such action as may be necessary to satisfy any policy conditions.

Executive Directors must inform the Director of Transformation Services and Performance of any vehicle acquisitions/disposals or premises acquisitions or disposals and of any occupations or vacations of premises.

Executive Directors are responsible for ensuring insurance renewal information is provided when requested annually by the Insurance & Risk team.

Back to Contents page

2.5.2. The Director of Transformation Services and Performance

The Director of Transformation Services and Performance will arrange the insurances considered necessary to cover risks to which the Council is exposed..

The Director of Transformation Services and Performance will periodically review all insurances in consultation with Executive Directors and determine the premiums to be charged as part of the Annual Budget process.

Back to Contents page

3. Financial Planning

There are 3 key elements to Financial Planning at Sheffield City Council:

- Medium Term Financial Strategy
- Annual Revenue Budget
- Capital Programme

Each element has a specific purpose and is designed to ensure the robustness of the Council's overall financial arrangements.

3.1. Medium Term Financial Strategy

The Medium Term Financial Strategy (MTFS) is a key requirement of good governance and is a key tool to help the Council deliver its priorities.

In line with the Leader's Scheme, the Cabinet is responsible for approving the Medium Term Financial Strategy and it will be refreshed and updated on an annual basis.

The Medium Term Financial Strategy links strongly to the Corporate Plan and the Corporate Plan drives the spending priorities that inform the Medium Term Financial Strategy. This will include allocating the overall expenditure limits for Community Assemblies.

The Director of Finance will be responsible for producing the Medium Term Financial Strategy in conjunction with Executive Directors and will recommend measures to the Executive that will support the Corporate Plan. This will be supported by policy options, savings and efficiencies, and both financial and non financial information to assist decision-making.

The Medium Term Financial Strategy will set an integrated financial plan for at least a three year period and will form the foundation of the Annual Revenue Budget and Capital Programme for the next year and projections for at least the following two years. This will include cash allocation or financial targets for Executive Directors for the forthcoming financial year and guideline allocations / targets for the following two years. The MTFS will also include projections of the Council's reserves and balances.

3.2. Annual Revenue Budget

The Annual Revenue Budget sets the detailed budget proposals for the Council for a one-year period and also sets the City Council element of the Council Tax for the following financial year.

Proposals and policy options for the Council's Annual Revenue Budget will be presented to Cabinet as part of the Medium Term Financial Strategy by the Director of Finance. The Director of Finance will then be responsible for preparing the detailed Annual Revenue Budget for the coming year in conjunction with Executive Directors.

Back to Contents page

Financial estimates will be produced for, and on behalf of Portfolios by the Director of Finance through Finance Business Partners. Executive Directors and the Director of Finance will work collaboratively to agree final spending proposals for inclusion in the Annual Revenue Budget.

The Director of Finance will advise on the inclusion of contingencies to cover exceptional in-year price movements and potential commitments which are uncertain either in terms of their financial impact or timing. Executive Directors will notify the Director of Finance of such items as part of the budget setting process so that an appropriate level of contingencies can be approved by the Council.

As part of the Annual Revenue Budget, the Director of Finance will be responsible for ensuring that the budget proposed meets relevant statutory requirements.

3.3. Annual Revenue Budget Approval

The Executive is responsible for agreeing the annual budget for services within Portfolios, including the overall capital programme, within the Budget and Policy Framework.

If agreed, the Executive will recommend the Budget to Full Council for final approval together with a recommended level of Council Tax to be set for the coming financial year.

As per Article 2 of the Council's Constitution the Council is required to set the Annual Revenue Budget and the appropriate level of Council Tax for the coming financial year by 11th March each year in line with statutory requirements.

Once the Annual Revenue Budget has been approved by the Council, Executive Directors may incur expenditure up to the amount approved for the period covered by that budget. Individual items of expenditure within the budget must still be approved in accordance with the Council's Standing Orders, Commissioning and Procurement Policy and any other relevant policies, and where the expenditure constitutes an executive function, in accordance with the Leader's Scheme.

Back to Contents page

3.4. Annual Revenue Budget Monitoring

3.4.1. Chief Executive and Executive Directors

The Chief Executive and Executive Directors, in consultation with the Cabinet Member for Finance, are responsible for taking appropriate action to ensure that the overall spending of the Council is within available resources.

Executive Directors must not overspend the approved Revenue Budget for their Portfolio and will be responsible for managing their approved Revenue Budgets within the cash allocations and financial targets approved by the Council, unless specific additional resources are provided by the Cabinet during the year.

Executive Directors must not make commitments relating to spending in future years without the agreement of the Director of Finance and consultation with the Cabinet Member for Finance. Any such commitments must be within the financial parameters set in the Medium Term Financial Strategy.

Executive Directors are responsible for ensuring that managers within their Portfolios work within the timescales and procedures stipulated from time to time by the Director of Finance.

The Executive Management team may recommend that budget monitoring information is presented to the relevant Overview and Scrutiny Committee in consultation with the Chair of that Committee.

3.4.2. Director of Finance

The Director of Finance will prepare budget monitoring reports in consultation with Executive Directors. The Director of Finance will produce an annual timetable for budget monitoring reporting and the following principles will apply:

- Monitoring reports, prepared on an accrued basis, will be reported to Portfolio Management Teams on a monthly basis.
- Monthly monitoring reports will be presented to Executive Management Team.
- Monthly overall monitoring reports will be presented to the Cabinet.

Monthly monitoring reports will be prepared for the portfolio holding Cabinet Member(s) by the Director of Finance in consultation with the Executive Director.

Consolidated monitoring reports will be presented to the Strategic Resources and Performance Overview and Scrutiny Committee if requested.

The relevant Overview and Scrutiny Committee of the Council may request more frequent budget monitoring information.

As soon as practical after the end of the financial year, the Director of Finance will report the overall Revenue out-turn position including details of reserves, balances and provisions held by Portfolios to Cabinet. The report should include recommendations relating to the treatment of any under and over spending by Portfolios.

Back to Contents page

3.5. Virements and Variations to the Annual Revenue Budget

3.5.1. Virements

Executive Directors are responsible for optimising resources and for managing their budgets prudently.

Virements are intended to enable the Executive and Executive Directors to manage budgets with a degree of flexibility, provided they remain within the Corporate Plan and the overall Budget and Policy Framework as determined by full Council.

Key controls for virements are that they must be approved in line with these Regulations, that they must not create additional overall budget liability, for example by creating future commitments from one-off additional spending and that both parties to the virement must agree to it.

Virements will not be permitted from capital financing charges, levies or other areas of spending as prescribed by the Director of Finance without the specific approval of the Director of Finance.

Virements requested by Community Assemblies will be proposed by the relevant Director and the process and limits below followed.

3.5.2. Variations

Variations are changes to the Council's overall level of resources as set out in the Revenue Budget Report that is approved by Council.

In accordance with Article 4.02f of the Council's Constitution, any decision about any matter **which would be contrary to or not wholly in accordance with the Budget** must be taken by Full Council. This requirement is subject to the urgency procedure in the Budget and Policy Framework Procedure Rules,

3.5.3. Approval of Virements between Services and Portfolios

Approval of the virement must be in line with the limits shown below and the Leader's Scheme:

- Under £500,000: the virement may be approved by the Director of Finance.
- £500,000 and Over: the virement may only be approved by the Executive in line with the Leader's Scheme

Where a virement would represent a major change of policy it must be approved in accordance with the Leader's Scheme regardless of its value.

If the cumulative effect of virements is over £500,000 during a financial year, these must be approved by the Executive (as above).

Back to Contents page

3.5.4. Approval of Virements between reserves and Portfolios

The principle criteria for assessing requests for carry-forwards or transfers to specific reserves is that the overall budget of the Portfolio making the request must be underspending, i.e. the Portfolio cannot exceed its approved budget.

Carry-forwards or transfers to specific reserves need to be linked to the annual revenue budget and business planning process and should therefore be identified as part of the business planning process. Requests must be done in line with the financial procedure on such matters.

Requests to carry forward underspends will require initial review by the Director of Finance and will be presented to the Executive as part of the monthly Revenue Budget Monitoring process. Approved requests will be included in the Budget Implementation Plan for the relevant Service.

Specific reserves may only be established by Executive Directors for future years' spending in consultation with the Director of Finance and will be presented to the Executive as part of the monthly Revenue Budget Monitoring process. Approved requests will be included in the Budget Implementation Plan for the relevant Service.

Revenue Budget allocations and Budget Implementation Plans are approved in accordance with the Council's Constitution

3.5.5. Approval of Variations

Any change to the overall level of available resources as set out in Budget must be approved by Full Council in line with the Council's Constitution.

Requests for variations may be submitted to the Council for approval as detailed below:-

- Under £500,000 **and** not representing a major change of policy: The submission of a request for the variation may be approved by an Executive Director in consultation with the Director of Finance and the relevant portfolio holding Cabinet Member.

- £500,000 and over **or** representing a major change of policy: The submission of a request for the variation may only be approved by the Executive in line with the Leader's Scheme

Variations to the Annual Revenue Budget that require Executive support will be proposed by the Executive Director and actioned by the Director of Finance.

Variations requiring Cabinet support will normally be presented to Cabinet as part of the normal budget monitoring cycle and in line with the requirements of the Leader's Scheme.

Any report to the Executive or to the Council recommending a variation to the Annual Revenue Budget must comply with Section 4 of these regulations in respect of the reporting and approval of Financial Implications.

Back to Contents page

3.5.6. Recording Virements and Variations

All approved Virements and Variations must be recorded on the Council's Finance System.

3.6. Borrowing and Investment (Treasury Management)

Only the Director of Finance may enter into any borrowing or investment on behalf of the Council.

The Director of Finance is responsible for formulating an annual Borrowing Strategy and Treasury Management Policy for approval by the Council in line with the Constitution .

The Treasury Management Policy and associated Treasury Management Practices will be issued and updated in accordance with all relevant legislation and recommended Codes of Practice.

The Director of Finance is responsible for providing an annual report to Council on treasury management activities, transactions and decisions over the preceding 12 months. The prime criteria for the effectiveness of treasury management activities is the identification, monitoring and control of risk. Therefore, the analysis and reporting of activities will focus on the risk implications for the Council.

In undertaking the Council's borrowing and investment operations, the Director of Finance will ensure compliance with the Borrowing Strategy, the Treasury Management Policy and all associated Treasury Management Practices.

Back to Contents page

4. Financial Implications

Executive Directors are responsible for ensuring that all reports to Cabinet, Individual Members, Scrutiny Committees, Community Assemblies and reports supporting Key Decisions by Officers include a section entitled ‘Financial Implications’. This section must summarise the capital and revenue expenditure implications of the proposals in the report together with any associated risks.

Although not mandatory, it is good practice to include a ‘Financial Implications’ section when reports are made to other meetings, e.g. less formal Member meetings, management teams etc. This will help to ensure that, from the beginning of the decision making process;

- the financial implications of decisions are given proper consideration,
- there is professional input from the officers in the Finance Service, and
- discussions and subsequent decisions take place with all the available information.

4.1. Sign–off of Financial Implications

The Director of Finance, or an authorised officer on his / her behalf, is responsible for signing off all Financial Implications summaries and, where applicable, the Appendices to the report.

Only the Director of Finance, as the budget holder for the Council’s Capital Financing costs, or Officers specifically authorised to do this on his / her behalf may approve Financial Implications which affect the cash-flow of the Council.

The Finance Service officer is responsible for ensuring that the Officer who has prepared the report has taken all relevant advice, e.g. specialist financial or taxation advice, before they sign off financial implications.

The name of the Finance Service Officer who has signed-off the financial implications must appear on the Financial Implications Section of the covering checklist.

Back to Contents page

5. Capital Programme

5.1. Background

5.1.1. <u>The Capital Programme</u>

The Capital Programme is made up of a number of schemes / projects which meet the definition of capital spending. It is the planned list of projects, together with supporting funds, that is agreed by Council in March each year and can cover the next 5 years.

The Programme is made up of a number of different elements which may change from time to time. This means that Capital Programmes may not be comparable in terms of size and scope over time.

Accounting for capital projects will be in accordance with current and approved International Financial Reporting Standards and the Statement of Recommended Accounting Practice (SORP).

5.2. Roles and responsibilities

5.2.1. <u>The Executive</u>

The Executive is responsible for ensuring that the Council's expenditure remains within the resources available to the Council. It is responsible for agreeing the Capital Programme before recommending it to Full Council, and for reviewing the monthly monitoring reports.

This responsibility extends to the approval of any requests for in year additions and variations to approved projects to the value stated in S5.3.4 (below) and as submitted through the guidelines laid down in these Regulations.

5.2.2. <u>Capital Programme Group</u>

The Capital Programme Group is responsible for;

- oversight of Capital Management,
- advising and making recommendations to the Executive Management Team on new project approvals. The recommendations will be made to Cabinet on a monthly basis,
- approving progress to next stage of delivery, variations to existing projects, and
- the use of capital receipts and grants.

Back to Contents page

5.2.3. Director of Finance

The Director of Finance is responsible for ensuring that capital projects are financially approved and reported in line with these Regulations and for producing a schedule (timetable) for reviewing, approving, managing and reporting capital spending.

In conjunction with the Executive Directors, the Director of Finance is responsible for approving Capital expenditure under the emergency approvals procedure.

5.2.4. Executive Directors

Executive Directors are responsible for ensuring that managers within their areas of responsibility comply with these Regulations and the procedures and timescales related to capital project management as defined by the Director of Finance.

They are also responsible for ensuring that managers adhere to the SCC Project Management Guidelines as appropriate.

In conjunction with the Director of Finance, the Portfolio Executive Directors are responsible for approving Capital expenditure under the emergency approvals procedure.

5.2.5. Directors and Project Managers

Directors and Project Managers are responsible for ensuring that the Council has the relevant legal authority to undertake a Capital Project and that all arrangements comply with these Regulations, Standing Orders, published Codes of Practice and relevant EU and domestic procurement rules.

Where consideration is being given to external funding for a capital project, either wholly or in part, Directors and Project Managers are responsible for complying with these Regulations and all associated procedures in relation to external funding.

5.2.6. Budget Managers

It is Council Policy that all projects are managed in accordance with the SCC Project Management Guidelines. These define a Project Manager as the officer who is responsible for the day to day running of the project on behalf of the Project Sponsor / Board. They are also responsible for delivery of the projects to cost, time and specification.

To avoid unnecessary duplication of terminology in these Regulations the term Budget Manager can also be read to mean Project Manager.

Budget Managers are responsible for considering revenue, environmental, property, and opportunity costs related to a project. They are also responsible for considering the legal, human resources, equalities impact and sustainability implications of the project.

Budget Managers must also consider the impact of Value Added Tax (VAT) on Capital projects and seek the advice of the Director of Finance if required. On a day-to-day basis this advice will be provided by the Council’s Tax Manager.

Back to Contents page

Budget Managers are responsible for managing the project to cost thus preventing overspends. They must consider the risks of, and the solutions to, any forecasted Capital overspends.

5.2.7. Business Partner (Capital) Team

The Business Partner Capital Team is responsible, alongside the Budget Manager, for steering a project through the financial approval process.

The Finance Business Partner Capital Team is also responsible for reviewing, quality checking and, where appropriate, challenging the Budget Manager's monthly review of actual and forecasted expenditure and income.

The Business Partner Capital Team is responsible for reporting capital expenditure and its financing in accordance with the Capital Projects Approval Hierarchy (see Section 5.3.4) on a monthly basis.

5.3. Capital Programme Approval

The proposed Capital Programme for the coming financial period is collated by the Director of Finance, in collaboration with Executive Directors.

The Programme must be reviewed by the Capital Programme Group prior to recommendation to the Executive Management Team then to Cabinet.

The agreed Programme must be presented annually, by the Director of Finance and the Executive Directors, to Full Council at the same time as the Annual Revenue Budget.

Inclusion of a project within the approved programme does not convey automatic authority for that project to commence.

The Annual Capital Programme report to Full Council will request delegated authority for the Director of Finance and the Director of Property and Facilities Management Services to;

- authorise approved projects within the programme to proceed through each stage,
- authorise how approved projects are funded,
- authorise reductions in the approved capital programme or constituent projects,
- authorise the issue and acceptance of tenders, subject to confirmation from Directors and Project Managers that a procurement professional has approved the issues and acceptance, and that all standing orders and regulations have been complied with.

The Budget Manager must obtain approval for each stage of design, procure, build, and completion through the delegated powers of the Director of Finance or the Director of Property and Facilities Management Services and the Capital Programme Group and in accordance with the provisions of the Leader's Scheme.

Back to Contents page

5.3.1. The Capital Approval Form

Financial Approval for projects within the Capital Programme, additions to the programme and variations to approved projects are facilitated through the Capital Approval Form (CAF).

A fully endorsed CAF, including all required documentation, which has been approved at Cabinet (or otherwise in accordance with the Leader's Scheme), gives authority to proceed with a project, subject to stage approvals.

The Capital Approval Form (CAF) requires the following endorsements (signatures):-

- for Annual Inclusions and Variations - the signatures of the Project Manager, sponsoring Director, and Finance Business Partner (Capital) Team

- for Emergency approvals - the signatures of the Project Manager, sponsoring Director, Finance Business Partner (Capital) Team, an Executive Director and the Director of Finance

- for cases considered sensitive by, or otherwise at the direction of, the Executive Director and / or the Director of Finance, the signatures of the Project Manager, sponsoring Director, Finance Business Partner (Capital) Team and the Individual Cabinet Member for the Portfolio.

5.3.2. Reports with financial implications

All reports with capital implications or other requests for approvals must be included within the capital programme approval process as described in these Regulations.

5.3.3. Project funding

Capital expenditure cannot take place unless it is fully funded or any funding gaps are approved by the Director of Finance.

In line with Section 6 of these Regulations bids for, or acceptance of offers of funding cannot take place until approved by either the Director of Finance or other authorised Finance Officers.

Authorisation should follow recommendations by the Capital Programme Group, taking account of the Council's resources, match funding availability and risk involved.

Funding cannot be recognised until all conditions for its receipt have been met. Before this point any shortfall against actual expenditure must be covered by either Portfolio revenue contributions to capital or by specific agreement for each project through corporate funding sources.

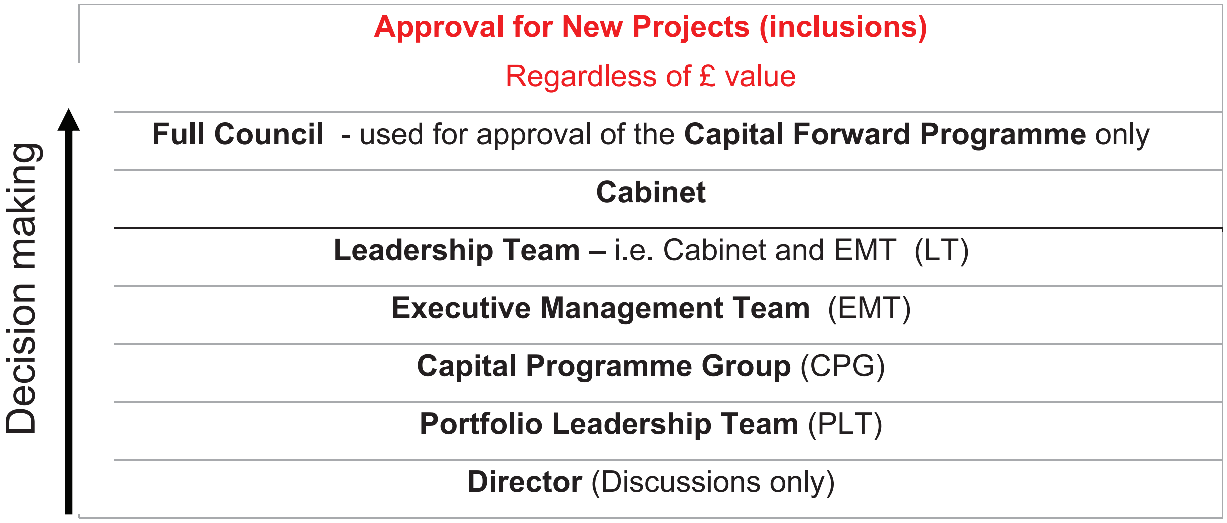
Capital Funding cannot be used to fund revenue expenditure.

Back to Contents page

5.3.4. Approval for New Projects / Inclusions / Changes

All new capital projects / inclusions in year and significant changes to the Capital Programme (other than changes requiring the approval of Full Council (Article 4 of the Constitution) must be approved by Cabinet or otherwise in line with the Leader's Scheme, and these Regulations. The approval chain is detailed below:-

Capital Projects Approval Hierarchy



Approval for New Projects (inclusions)

Regardless of £ value

Full Council - used for approval of the **Capital Forward Programme** only

Cabinet

Leadership Team – i.e. Cabinet and EMT (LT)

Executive Management Team (EMT)

Capital Programme Group (CPG)

Portfolio Leadership Team (PLT)

Director (Discussions only)

5.3.5. Variations to projects in the Capital Programme

Changes to a project's finance require approval as a 'Variation' subject to necessary capital resources being available.

Variation Approval levels on an existing approved project are as follows:-

- A variation in cost of up to £25k can be approved by the responsible Director
- A variation in cost between £25k and £100k requires EMT approval
- All other variations require Cabinet approval through the monthly monitoring report

For authorisation purposes, Variations are measured cumulatively from the last approval by the Executive.

5.3.6. Emergency approvals

Where an emergency approval is required, this must be provided in accordance with any applicable urgency procedures in the Constitution or the Leader's Scheme. Any such approvals shall be reported retrospectively to Cabinet in the next monthly report by the relevant Executive Director and the Director of Finance.

Emergency approvals can be rescinded by the Cabinet.

Back to Contents page

5.3.7. Virements

Virements are not permitted between Capital schemes. Changes from Cabinet approved amounts must be treated as Variations.

5.3.8. Slippage and / or accelerated spend

Where the timing of expenditure deviates from the annual profile approved by Cabinet, Budget Managers should reflect this in their monthly forecast and advise Finance Business Partner Capital of the situation.

Where the forecast has changed such that expenditure will move between financial years, the monthly report to Cabinet will seek approval for this change.

5.3.9. Change in Scope

Where material output from the project will be different from that of the last approved Executive authority, Budget Managers must seek new Executive approval.

5.3.10. Revenue implications

The revenue expenditure implications of the proposed Capital Programme will be considered as part of the approval process outlined in these Regulations and as part of the Annual Revenue Budget and Medium Term Financial Strategy processes.

Where a Budget Manager identifies that the project will overspend even after all mitigating action, and that no alternative capital funding source is applicable, then the overspend must be made good from revenue funding.

5.3.11. Capital Receipts

Any decision on the use of Capital Receipts will be taken as part of the overall approval for the project through recommendation by the Capital Programme Group as outlined in S 5.3.4 above.

Any use of Capital Receipts must first be reviewed by the Asset Management Group as part of the development of the proposed Capital Scheme.

5.3.12. Project Stage Approval

Approval for the Design, Procure and Build stages of a project will not be granted without recommendations from the Director of Finance in respect of funding implications. As part of this process the Director of Finance will need to consider both the Revenue and Capital implications of such approvals for the level of contractual commitments in future years.

The Budget Manager must obtain approval for each stage of design, procure, build, and completion through the delegated powers of the Director of Finance or the Director of Property and Facilities Management Services and the Capital Programme Group.

Back to Contents page

The build stage of a project cannot proceed until a thorough review has been produced by the Project Manager, approved by the appropriate sponsoring Director and reported to the Capital Programme Group. In line with the Council's Project Management Guidelines, a Project Review must be undertaken and appended in support of the submission for project stage approval.

Executive Directors and Directors must ensure that agreed formal procedures are in place with the Head of Design and Project Management and the Director of Commercial Services in respect of all procurement related to capital projects.

5.4. Financial Management and Reporting of Capital accounts

5.4.1. Financial Management

Inclusion of a project in the Capital Programme and its subsequent progression to completion will be managed through the use of the Council's financial management system.

In line with the requirements of these Regulations, Budget Managers are required to carry out a monthly monitoring and forecasting process in respect of the 'actual to date' and 'forecast 'position for both revenue and capital accounts.

5.4.2. Reporting

The Director of Finance is responsible, with Executive Directors, for providing a consolidated monthly report to the Executive in relation to Capital accounts.

Monthly capital reporting will be based on Capital Approval Forms (CAF), Project Closure Forms (PCF), financial monitoring and approval request reports.

At year end the Director of Finance will report to the Executive the overall Capital Out-turn position at the same time as the Revenue Out-turn position is reported to the Executive.

Back to Contents page

6. External Funding / Grants

6.1. Background

External Funding in its broadest sense refers to the identification and securing of additional resources, above and beyond those normally provided to organisations, which enables them to develop and enhance the quality of their services, better meet the needs of clients and to do something that could not otherwise be achieved.

The Council relies on a significant amount of external funding to finance the service activity and specific projects / programmes needed to meet its six ambitions as highlighted in the Corporate Plan.

6.2. Roles and responsibilities

6.2.1. The Director of Finance

The Director of Finance is responsible for ensuring that:-

- There are proper processes and procedures in place for the completion, authorisation and submission of applications for external funding and any subsequent claims. In practical terms this responsibility is discharged through the External Funding Team which is part of the Shared Service function within the Finance Service,
- grant applications are correctly completed and submitted by the required date with a view to maximising the income to the Council in terms of cash flow,
- all completed grant claims and certifications are approved by the Director of Finance or other authorised Finance Officer as published in the Financial Protocol (Appendix A to these Regulations) and maintained by the Director of Finance,
- all documentation related to match funding, e.g. certificates, letters of comfort, heads of terms, contracts, is approved by the Director of Finance or other authorised Finance Officers as published in the Financial Protocol,
- all statutory financial returns related to external funding are completed and submitted in line with relevant guidelines,
- the income due from grant claims is received, and
- records are kept for the reconciliation of grants due and received. Such records must have robust audit trails and meet External Audit requirements.

Back to Contents page

6.2.2. Executive Directors

Executive Directors are responsible for ensuring that;

- all available external funding is claimed. In practical terms this responsibility will be discharged by the Directors and Budget Managers within the Portfolio,
- all applications for external funding within their area of responsibility are made in line with all the processes and procedures laid down by the Director of Finance,
- all the funding body's conditions and criteria are met and can be fully evidenced
- grant claims are prepared and submitted as required,
- where the City Council is providing match funding, all documentation as required by the funding body is duly authorised by the Director of Finance, or other authorised Finance Officers as published in the Financial Protocol. Documentation includes but is not confined to Match Funding Certificates, Letters of Comfort and Heads of Contract,
- risks to the Council are appropriately identified, recorded and managed,
- any legal implications and risks of working with partners are appropriately addressed,
- all required evidence related to the external funding body's qualifying conditions and / or criteria is collected and retained as appropriate,
- all external funding within their area of responsibility is managed using the Council's systems and processes.

6.3. Grant / External Funding accounting

All accounting processes related to external funding / grants will be controlled by the External Funding Team in the Shared Services Function of the Finance Service.

6.4. Audits of external funding

Audits of external funding shall be carried out in accordance with the conditions / criteria related to the funding.

Where there is a charge for the audit this is payable from the relevant Business Unit's budget.

6.5. Retention of documentation

All evidence required by the funding body must be collected and retained in line with the conditions / criteria related to the funding.

Where the retention period in the agreement exceeds the one prescribed in the Financial Records Retention Schedule, (see Appendix C) the funder's requirements will take precedence. As an example, ERDF requires documentation to be retained 12 years after **closure** of the Programme.

Where the retention periods required by the funder are less than those specified in the Financial Records: Recommended Retention Schedule (Appendix C of these Regulations) the latter should be followed.

Back to Contents page

7. Income Management

This section covers the principles that apply to setting fees and charges, the collection of income, raising of sundry debtor accounts and debt recovery.

Separate detailed rules apply to the management of Housing Rent, Council Tax, Business Rates and Benefit Overpayment debt and are therefore not covered by these Regulations.

7.1. Roles and responsibilities

7.1.1. The Executive

In accordance with the Leader's Scheme, the Executive is responsible for agreeing the overall charging policy for fees and charges levied by the Council even if the actual level of the charge is set by an outside body i.e. Government. In this context Fees and Charges excludes Council house rents, Council Tax, National Non-domestic Rates and Housing Benefit overpayments.

Fees and charges must be set as part of Business Planning process and in line with the provisions of the 'Fair Fees and Charges' Policy as approved by the Executive. Recommendation of changes to fees and charges should be made as part of the Annual Revenue Budget Report to Council.

Any changes in Fees and Charges that are not approved as part of the Annual Revenue Budget Report to Council must be approved in line with the requirements of the Leader's Scheme.

7.1.2. Individual Cabinet members

The Leader's Scheme may provide for Individual Cabinet Members having responsibility for agreeing changes to existing fees and charges in relation to their Portfolio areas.

7.1.3. Executive Directors

Executive Directors are responsible for seeking, where appropriate, to recover the full cost of their services through setting fair fees and charges in line with the provisions of the 'Fair Fees and Charges' Policy and all other statutory guidance.

Executive Directors are responsible for having arrangements in place for payment up front wherever possible and for having appropriate arrangements for the storage and banking of cash.

They are also responsible for ensuring adequate security arrangements for the storage and transportation of cash and requesting insurance cover. They must also immediately inform the Police, Internal Audit and the Insurance and Risk Team where any theft of cash or its equivalent is discovered or suspected.

Back to Contents page

Where accounts are raised in respect of charges for works done, goods supplied or services rendered on behalf of the Council and all other income due to the Council, Executive Directors are responsible for ensuring that they are raised and issued to the customer(s) within the required timescales and in accordance with these Regulations and all associated policies and procedures.

To effect this, Executive Directors are responsible for ensuring that their staff receive training and follow the published guidance on invoice raising.

Executive Directors are responsible for effectively managing the level of debt within their Portfolio, including resolving disputes within the required timescales, identifying debts that are clearly irrecoverable and authorising them to be written off.

They are also responsible for ensuring that all relevant documentation related to the supply is retained and accessible in the event of it being required for debt recovery procedures, up to and including court action.

Income and Sundry debt processes can be susceptible to money laundering activities. Executive Directors are responsible for ensuring that their staff are aware of this possibility and that they comply with the Council's Anti – Money Laundering Policy.

7.1.4. Director of Finance

The Director of Finance is responsible for developing and maintaining a sundry debt income collection policy on behalf of the Council. The income policy will take account of such factors as statutory obligations and related Council policies and will be subject to regular reviews.

The Director of Finance is responsible for determining the methods that may be used to collect income and for providing training and advice on these methods.

The Director of Finance is responsible for providing training and advice on the raising of invoices. On a day-to-day basis this responsibility is discharged by the Financial Systems Support Group in the Finance Service.

The Director of Finance is responsible for all debt recovery actions except Housing Rents. In respect of sundry debt this responsibility is discharged by the Central Debt Recovery Team in the Finance Service.

In respect of local taxation and Housing Benefit overpayment debt this responsibility is discharged by the Revenues and Benefits Team within the Finance Service

The Director of Finance is responsible for providing advice on best practice for cash storage and banking.

The Director of Finance is also responsible for receiving disclosures about Money Laundering activities within the Council

Back to Contents page

7.1.5. The Director of Transformation Services and Performance

The Director of Transformation Services and Performance is responsible for providing insurance cover for cash and cheques awaiting banking as requested by Executive Directors.

7.1.6. All officers involved in the sundry debt process

Officers responsible for raising invoices, credit notes, refunds, debt recovery and write-offs must not do so for debt to themselves, family members, or where they have a vested interest.

7.1.7. Separation of duties

The system adopted for the collection and banking of income must incorporate separation of duties between the different functions as a principal form of internal control.

To comply with this principle the Budget Manager must ensure that no one officer is responsible for more than two of the functions within the boxes shown below and must not be responsible for functions in both boxes.

- Identification of charges or booking
- Billing.
- Collection and receipt of income.

- Reconciliation of receipts to income.
- Banking.
- Monitoring of balances received, banked and outstanding.

All transfers of money between members of staff shall be evidenced by the recorded signature of the officer receiving the money.

7.2. Payment of fees and charges

7.2.1. Payment Up Front

Wherever possible the provision of credit, i.e. payment via an invoice, should be avoided and, if appropriate, customers asked to pay for services up-front or at the time of service delivery. This avoids the need for invoicing thus reducing both the potential for invoices not being paid by customers and administration costs to the Council.

The Director of Finance will determine standard methods for taking payments for goods or services. These must be used by all Services and partner organisations as determined by the Director of Finance

Payments cannot be made by any other means except by express permission of the Director of Finance.

Back to Contents page

Where there are significant cash payments, i.e. £1,000 or more in cash, or up to £2,500 in linked transactions, officers should check the identity of the client in line with the Council's Anti – Money Laundering Policy.

Payments in cash must not be accepted by employees of the Council or any of its agents where the amount is over the limit to be determined by the Council's Money Laundering Reporting Officer. Currently the limit has been determined as £2500.

7.2.2. Payment by invoice

Payment by sundry debt invoice is, in effect, providing credit to the customer. This must be avoided wherever possible and invoices must only be raised where payment in advance or at the point of service delivery is inappropriate.

All sundry debtor accounts must be raised on the Accounts Receivable section of OEO finance system unless exceptions have been agreed with the Director of Finance.

Invoices should be issued within 10 working days of the;

- goods or services being supplied,
- month end where there is an on-going service provision, or
- bill becoming due for payment.

To comply with all relevant HM Revenue and Customs regulations the date of the invoice must be within 60 days of the actual date of supply. Where this timescale cannot be met, advice must be sought from the Council's Tax Manager.

The information on the Sundry Debt invoice must be correct, complete and supported by all necessary and relevant information. In the event of debt recovery action being taken, up to and including Court proceedings, this information will be required as evidence. Officers raising invoices are also responsible for ensuring that the correct VAT treatment is applied.

To ensure that invoices are raised correctly, they must only be raised by officers who have had appropriate training.

Back to Contents page

There are standard methods for customers to pay sundry debt invoices and these are listed on the back of the invoice. These methods are currently;

- Cash, cheque or Debit card at a Post Office
- Cash at a PayPoint outlet
- Debit or Credit Card over the telephone
- Over the internet (on-line)
- By BACS

These must be used by all Services and partner organisations as determined by the Director of Finance.

In line with standard accounting practice, income will be credited to the relevant Business Unit at the point the invoice is raised - not when it is actually received.

7.2.3. Credit Notes and Refunds

Credit notes are required for an invoice that has been incorrectly raised. However, credit notes represent a control risk and as such must be properly authorised. Credit notes must be authorised jointly by the manager responsible for the budget affected and the Director of Finance or his / her designated Officers.

Refunds are required if a customer or other member of the public has paid an incorrect invoice or has paid money into a Council bank account in error. Refunds may only be actioned by the Director of Finance or his / her designated Officers.

Where a refund is for a significant amount, i.e. £1,000 or more, officers should check the identity of the client in line with the Council's Anti – Money Laundering Policy.

7.3. Fees and interest charges

Individual Business Unit will not be charged for payments by credit card. The maximum amount allowed in a single transaction by credit card is £2500.

Interest on late payment of debt by commercial customers will be applicable where agreed by the Director of Finance.

Back to Contents page

7.4. Banking of collected income

7.4.1. Receipting and banking

All income received on behalf of the Council must be receipted and paid into the appropriate bank account without unnecessary delay and in accordance with the procedures approved by the Director of Finance for the banking of income.

Income must be paid in without deduction unless this is approved by the Director of Finance. Third party and personal cheques must not be cashed from monies held on behalf of the Council.

7.4.2. Safe storage of collected income

Executive Directors are responsible for ensuring that all income collected prior to banking is safeguarded and that adequate insurance cover has been arranged.

The amount of cash allowed to be held in any one safe overnight will vary according to the particular insurance arrangements. Where the agreed limit is likely to be exceeded then arrangements must be made to bank the income as soon as possible.

The Director of Finance will advise on best practice for cash storage and banking.

The Director of Transformation Services and Performance is responsible for providing insurance cover for cash awaiting banking as requested by Executive Directors and providing the insurance cover requested by Executive Directors.

7.4.3. Reconciliation of receipts

Reconciliation of receipts to banked income should be performed on a regular basis and at least monthly, reflecting the value of the receipts. Staff responsible for reconciliation should not be involved in day to day banking or receipting procedures.

7.5. Debt Recovery

7.5.1. Recovery process

The Council’s standard payment terms and conditions are that, unless contractually agreed or in the case of a demand payable by installments, sundry debts are payable immediately and in full.

The Council will undertake robust action up to and including Court action to recover money owed to it. The costs of enforcement action to recover sundry debts, up to and including court action will be borne by the relevant Business Unit.

Back to Contents page

7.5.2. Arrangements to Pay

Where a customer is unable to pay the full amount of a sundry debt invoice immediately then arrangements can be negotiated, in appropriate circumstances, to clear the debt in the shortest possible timescale.

These arrangements can be negotiated by the Central Debt Recovery Team in consultation with the Business Unit Manager, or directly by the Manager. In the latter case the Business Unit Manager must inform the Central Debt Recovery Team so that the arrangement can be documented and monitored.

Payment arrangements that exceed 12 months must be agreed by the Director of Finance.

If the arrangement to pay is not maintained then debt recovery action will be commenced or continued.

7.5.3. Disputed debts

For the purposes of these Regulations a ‘dispute’ relates to an issue that must be resolved before the customer will pay an outstanding sundry debt.

When a debt is put into dispute, debt recovery action is suspended to allow time for the issue to be resolved.

The relevant Business Unit Manager is responsible for resolving the dispute and for doing so within 28 days. Where the Business Unit Managers considers that a longer timescale is required to resolve the dispute, they must contact the Central Debt Recovery Team to request an extension. The request must be supported by details of the customer, the nature of the dispute and the extra length of time required must be specifically stated.

Back to Contents page

7.6. Bad and Doubtful Debt Provisions

When an invoice is raised the Business Unit is immediately credited with the income. For that income to be relied upon the debt must be paid within 60 days.

If a debt is not paid by day 60, a charge will be made against the Business Unit to make full provision for the debt not being paid. Exceptions to this are where the;

- debtor has an agreement to pay and is abiding by it
- debt is covered by a Charge (e.g. on property, land etc.)

Creating a provision for bad or doubtful debt does not mean that recovery action will stop. The Council will continue to take recovery action after the provision is made.

7.6.1. Payments received after 60 days

Where an outstanding debt is paid after day 60 and before day 91 the Business Unit will be credited with 50% of the income. The remaining 50% will be diverted to help balance the Council’s overall budget.

If the debt is paid after day 90, 100% of the income will be diverted to help balance the Council’s overall budget and the Business Unit will not receive any.

Exceptions to the ‘60 day rule’ can only be approved by the Director of Finance. A list of the agreed exceptions is maintained by Central Debt Recovery Team in the Finance Service.

7.7. Bad Debt Write-offs

If recovery action is unsuccessful, the Council may write-off debts that are correctly due to it but which, for whatever reason, are no longer collectable

All possible recovery procedures should be pursued and exhausted within 12 months of the invoice date. After this timescale the outstanding debt should be written off unless;

- it is covered by an on-going payment arrangement
- there is on-going action, up to and including Court action, to recover the debt
- the debt has been recorded on the Local Land Charges Register.

Writing off a debt involves removing a debt from the Council’s accounts using money that has been set aside as part of the bad and doubtful debt provision and will only be done in exceptional circumstances.

Write-offs must be proposed by the relevant Executive Director and approved and actioned by the Director of Finance.

By the time a debt is written off a full provision must have been created for it and reported to Members as part of the monthly budget monitoring process.

Back to Contents page

8. Purchasing

This section covers the principles related to procurement in the Council, the roles and responsibilities of officers and the principles that apply to the Council's Purchase to Payment (P2P) process. These are standard across all portfolios and must be complied with, unless an exception has been approved in writing in advance by the Director of Finance.

All Orders for goods or services are to be placed on the Council's Finance system or other systems as approved by the Director of Finance. Irrespective of the system used, the controls and processes detailed in these regulations will apply.

All procurement must comply with Contracts Standing Orders and the Leader's Scheme of Delegation of Executive Functions,

8.1. Roles and responsibilities

8.1.1. Director of Commercial Services

The Director of Commercial Services is responsible for ensuring that the Council's Standing Orders remain technically correct, up to date and fit for purpose.

The Director of Commercial Services is responsible for ensuring that the Council's Standing Orders are adhered to and all unauthorised breaches must be reported to him / her.

All requests for a waiver of Standing Orders must be made through the Director of Commercial Services.

The Director of Commercial Services is responsible for ensuring there are proper processes and procedures in place for the commissioning and procurement of goods and / or services, for providing advice and guidance on the procurement process and for ensuring that training and guidance is available for officers involved in the P2P process.

The Director of Commercial Services is responsible for approving suppliers used in the commissioning and procurement of goods and / or services.

8.1.2. Director of Finance

The Director of Finance is responsible for ensuring that VAT related records e.g. invoices or credit notes, are stored and made available in line with H.M. Revenue and Customs (HMRC) directives.

The Director of Finance will ensure compliance with the requirements of the Construction Industry Tax Deduction Scheme (CITDS) in relation to the payment of invoices relating to repairs and renovation over the stipulated monetary limits.

The Director of Finance will ensure that, where required, employment status of individuals are validated and all related records are stored and made available in line with HMRC directives.

The Director of Finance is responsible for the approval and administration of all leasing and other credit arrangements. Records will be kept by the Director of Finance of all relevant financial information relating to these arrangements.

Back to Contents page

8.1.3. Director of Finance and Executive Directors

The Director of Finance and Executive Directors are responsible for ensuring that all purchasing within their area of responsibility complies with the following principles:

- Expenditure shall not be incurred where it represents a departure from Council policy or where it is not in accordance with the approved Budget unless such expenditure is considered a matter of urgency. In these cases the Director of Finance must be consulted before incurring such expenditure.

- Where any consents are required from a Government Department or other relevant body, these shall be obtained before any expenditure or commitment is incurred.

- Appropriate controls must be in place that ensure the integrity of expenditure incurred in the name of the Council and constrains expenditure to within the legal powers of the Council.

The Director of Finance and Executive Directors are also responsible for ensuring that purchasing to payment arrangements within their area of responsibility comply with;

- these Regulations
- the Council's Constitution, and Leader's Scheme of Delegation of Executive Functions,
- Standing Orders for Contracts,
- Procurement policies
- The Guide for the Procurement of Consultancy
- HMRC requirements for checking employment status of individuals or groups of workers
- Corporate financial policies and standards
- EU and domestic law,
- Health and Safety Regulations
- Environmental Policy

The Director of Finance and Executive Directors will be responsible for ensuring that all suppliers providing services to the Council have the necessary HMRC certification enabling them to be paid through the Council's payments system. Contractors failing to comply with the conditions or to provide evidence of the necessary certification should be set up as temporary employees of the Council and paid through the payroll.

Back to Contents page

8.1.4. Budget Managers

Budget Managers with responsibility for incurring expenditure on behalf of the Council must ensure that the Council is obtaining value for money and that all expenditure complies with the Council's Contracts Standing Orders.

Budget Managers are responsible for ensuring that In–House and Corporate Contract providers are used wherever possible. Where this is not considered appropriate, advice must be sought from Commercial Services on choosing an alternative supplier and Contracts Standing Orders must be complied with.

Budget Managers are responsible for documenting and retaining evidence of compliance with Council's Contracts Standing Orders and all relevant procurement processes.

Budget Managers must ensure that any relationships with existing or potential Council contractors are declared prior to the obtaining of quotations or the awarding of contracts.

8.1.5. All Officers involved in P2P process

All officers involved in the ordering and purchasing processes must refer to the Council's Contracts Standing Orders for details of procurement procedures to be followed, with special attention to the need to use In–House and Corporate Contract providers.

Officers must formally declare any relationships with existing or potential Council contractors prior to the obtaining of quotations or the awarding of contracts.

Officers must withdraw from any P2P process when either they themselves or a member of their family of one of their close associates are involved directly or indirectly with the transaction.

Officers' attention is drawn to the provisions of Section 117, Local Government Act 1972, under which certain failures by an Officer to declare an interest in a contract with the Council may be punishable as a criminal offence.

8.2. Ordering of goods and services

A purchase order is required for all purchases of goods and services and one must be processed before requesting the supply.

Exception to this would be for the payment of utilities, recurring payments, 'multiple' and 'one-off' payments.

Verbal orders must not be used in normal Council operations and should take place only in wholly exceptional circumstances. Any verbal orders must be followed immediately by the issue of a fully authorised order. Officers making verbal orders can expect to be asked to support their decision by the Director of Finance and Director of Commercial Services.

Different Purchase Order types are in place to meet expenditure requirements including those that are not for the supply of goods or services

Orders must fully detail the goods and services to be supplied and the budget from which the expenditure is to be met. Final costs or an estimate of the costs of the goods or services ordered (net of VAT) should also be provided.

Back to Contents page

Orders must only be raised for goods and services provided to the Council or on official Council business. Individuals must not raise official orders for their own private use.

Variations must only be actioned through properly authorised amendments to orders. Issued orders must not be amended verbally with the supplier.

8.3. Authorisation of expenditure

8.3.1. Purchase Orders

Before authorising an order, Approvers must ensure that the proper approval for the spending has been obtained in line with the Council's decision making framework. In other words, the decision to spend the money must have been taken by Council, the Leader, Cabinet, a Community Assembly or a committee, an individual Member or Officer exercising delegated powers.

These Officers must also ensure that the Council's procurement rules and Standing Orders have been complied with before approving any order.

Authorisation in accordance with the requirements set out below is not a substitute for formal approval as required by Leader's Scheme, the Council's Standing Orders and Procurement Policy

Before authorising an order, managers, who must have written delegated authority from the Head of Service, should be satisfied that:-

- the Order represents legitimate liabilities of the Council,
- the required checks have been evidenced,
- sufficient budgetary provision exists to cover the payment,
- the expenditure is correctly coded, and
- all necessary documentation is attached

8.3.2. Authorisation to pay Utility Bills,

These will be authorised in line with the procedures as approved by the Director of Commercial Services and the limits as detailed in the Authorisation Matrix below.

8.3.3. Authorisation of Recurring, Multiple, One-Off and Foreign Payments

These will be authorised in line with the procedures as approved by the Director of Finance and the limits as detailed in the Authorisation Matrix below.

Back to Contents page

8.3.4. Authorisation Matrix

The list of Officers authorised to approve Purchase Orders will comply with this section of the Regulations and will be held in the Council's Finance System or other systems as approved by the Director of Finance.

All purchase orders must be approved in line with the Council's authorisation matrix as shown below.

Order Amount	Authorisation Level
£0 - £249	Supervisor / Line Manager
£250 - £499	Middle Manager
£500 - £2,499	Business Unit Manager
£2,500 - £24,999	Assistant Head of Service / Assistant Director
Over £25,000	Head of Service / Director / Asst Chief Executive / Chief Executive
Orders over £250 must also be reviewed by the Council's Commercial Processes Team to ensure compliance with Council Standing Orders etc	

The values in this matrix are set at levels deemed necessary by the Director of Finance for the proper control of expenditure.

Where, after consultation, the Director of Finance considers that the values should be revised in order to maintain that control, she / he may change them at any time.

For the avoidance of doubt, this matrix will apply to all orders including orders connected to the spending of Grant funding, contract payments and partnership arrangements where the Council's finance system is used to make a payment.

The existence of a Cabinet report approving a grant payment or awarding a contract does not over-ride the authorisation matrix.

This matrix will also apply to the authoriation of payments detailed above which do not require a Purchase Order.

Back to Contents page

8.4. Delivery of Goods and Services

Deliveries of goods and services should be checked to ensure that they are in accordance with the official order, taking account of, as a minimum;

- cost
- quantity
- quality, and
- fitness for purpose

Delivery notes must be retained for verification purposes in accordance with the Financial Documents Retention Schedule appended to these Regulations.

Officers are required to enter a receipt on the council's finance system, or other systems, as approved by the Director of Finance to confirm delivery of the goods or services.

8.5. Payments to suppliers

8.5.1. Supplier invoices

Suppliers will be expected to provide an electronic invoice through the Council's procurement system.

Where paper invoices are unavoidable these should be sent directly to the Council's outsourced provider of the accounts payable service for prompt processing and on no account should they be sent directly to the service requesting the supply.

Failure to adhere to this rule may result in delays to the payment process.

Any paper invoices will be scanned and attached to the invoice records by the outsourced provider of the accounts payable service.

8.5.2. Payments

No payment will be made unless supported by an appropriately authorised and receipted Purchase Order. Exceptions to this are Recurring, Multiple, One-Off and Foreign Payments as described above.

Where the details on both the supplier invoice and the receipted order are the same, or within tolerance levels agreed by the Director of Finance, the automated matching process will clear the invoice for payment in accordance with the Council's standard payment terms.

Where the details are not the same and are outside the agreed tolerance levels, then the order raiser should either raise a returns note in the P2P system or request a credit note from the supplier to resolve the mismatch.

Back to Contents page

8.5.3. Standard payment terms

The Council's standard payment terms are 30 calendar days from the date that a valid invoice is received by the Council. Any variation to this standard must be agreed by the Director of Commercial Services either as part of the letting of a contract or by ad-hoc exception to the standard terms.

In accordance with the Council's Standing Orders (C.4.7) advice must be sought from Director of Commercial Services where a supplier makes a request for payment in advance.

Back to Contents page

9. Internal charges

The Council's internal charging system covers;

- specific ordering and the consequent recharges
- Agreed Annual Service Level Agreements and the consequent recharges
- Overhead apportionment.

A fundamental requirement of the internal charging system is that both customers and suppliers are clear that the system is in operation and that they adhere to the relevant procedural guidance.

9.1. Roles and responsibilities

9.1.1. Executive Directors

Executive Directors are responsible for ensuring that their managers and staff follow the procedures relating to internal charges, including the requirement for an internal order and the use of specified financial codes.

9.1.2. Director of Finance

The Director of Finance is responsible for ensuring that there are proper processes and procedures in place to support the internal charging system, including details of specific financial codes.

10. Payroll, Expenses and Petty Cash Floats

10.1. Roles and responsibilities

10.1.1. Executive Directors

Executive Directors are responsible for ensuring that payroll information is correct and that information is provided within the agreed timetables for the running of the payroll.

They are also responsible for ensuring that all amendments to the payroll, e.g. Post and Establishment changes, individual contract changes etc, are notified in line with the procedures as approved by the Director of Human Resources.

Executive Directors are responsible for ensuring that all payments to employees are made through the payroll, that they are made only to official employees, that they are in accordance with individual contracts of employment, and that all necessary information is supplied so that deductions including PAYE and Superannuation are properly administered.

Executive Directors must ensure that when payroll costs are checked this is done so by officers not responsible for amendments to the payroll.

Executive Directors are responsible for determining any petty cash requirements for their Portfolio subject to approval by the Director of Finance or one of his/her authorised officers. This amount should represent a balance between the need for ready access to cash for small local payments, the risk of holding cash on the premises and the security arrangements required.

They must ensure that procedures are in place to formally assign responsibility for all floats and that the officer is properly trained in the administration of the float.

Back to Contents page

10.1.2. Director or Human Resources

The Director of Human Resources is responsible for approving and controlling arrangements for the payment of all salaries, wages, pensions, expenses and any other payments to all employees and former employees of the Council.

10.1.3. Director of Finance

The Director of Finance is responsible for approving the arrangements for payment of all salaries, wages, pensions, expenses etc made by the Director of Human Resources.

The Director of Finance is responsible for formulating and approving procedures related to Payments to Individuals and the Administration of Petty Cash Floats. S/he is also responsible for approving changes to the accounting and taxation elements of the payroll system.

10.2. Payroll

The payment of all salaries, wages, pensions, expenses and any other payments to all employees and former employees of the Council must only be made under arrangements approved and controlled by the Director of Human Resources and approved by the Director of Finance.

Amendments to the payroll, e.g. for absences and variations to pay, shall be limited to those Officers authorised to do so.

Payment of fees to individuals who are not Council employees must be made through the Purchase to Payment system and in accordance with the requirements of HM Revenue and Customs and the relevant procedures as laid down by the Director of Finance and the Director of Commercial Services.

Payment and personnel records must be held securely.

10.3. Expenses

Members and officers will only be entitled to travel, subsistence and incidental expenses where these are incurred legitimately in performing duties on behalf of the Council in line with the agreed policy and rates. Claims should be made in line with relevant Council policies including the requirement to forward receipts to the Council's outsourced provider of the payroll service. All such payments will be made through the payroll system.

Payments of expenses to individuals who are not Council employees must be made through the Purchase to Payment system in accordance with the procedures as laid down by the Director of Finance.

Expenses incurred by agency staff should be included in the Agency charge and paid through the Purchase to Payment system.

Back to Contents page

10.4. Petty Cash floats

10.4.1. Payments from a float and re-imbusements

The use of monies from petty cash floats must be limited to non-payroll related expenditure up to a maximum of £25 for which there is proper authority and provision in the budget but which do not justify an order being raised through the Purchase to Payment system. Petty cash should not be used for the payment of regular suppliers other than in exceptional circumstances, when prior approval must be obtained from Heads of Service.

Wherever possible purchases should be made in advance and, if applicable, VAT receipts provided before the petty cash is issued.

At the manager's discretion, a maximum of £5 employee related expenses may be paid from a petty cash float where an employee has been requested to travel to meet a service need and has no way of funding this.

Personal or third party cheques must not be cashed or money borrowed from petty cash floats. Private monies are not to be used to supplement the floats

Cash income from other sources must not be used to reimburse petty cash unless specific arrangements are in place.

10.4.2. Responsibilities of the float holder

Officers who have been assigned responsibility a float must ensure that they follow the procedures related to the administration of petty cash floats as laid down by the Director of Finance.

10.4.3. Personal credit card transactions

The use of personal credit cards by officers for petty cash transactions shall be limited to **exceptional** circumstances where petty cash would be appropriate but is not available.

Back to Contents page

11. Bank accounts and credit cards

11.1. Bank Accounts

Bank accounts in the name of the authority may only be opened and / or closed with the authority of the Director of Finance. This includes associated bank accounts which the Council does not directly control, e.g. joint arrangements etc. The Director of Finance is responsible for all negotiations of banking terms with the Council's Bankers.

All stand-alone systems which actually create payments and do not interface with the financial ledgers must have a separate bank account and consequent local reconciliation responsibilities. These are the Payroll interfaces, and systems which create BACS files or print cheques.

11.2. Reconciliations

Bank reconciliations should be completed on at least a monthly basis by an officer who is not responsible for the processing of payment and receipt transactions through the bank accounts. The Director of Finance is responsible for ensuring that reconciliations, together with supporting documentation, are reviewed and appropriately certified.

11.3. Banking transactions

The Director of Finance is responsible for maintaining an authorised signature list for Banking Transactions. The authorised signatories will be determined and approved by the Director of Finance in consultation with the Individual Cabinet Member for Finance. Authorised Signatories will normally be senior Officers who report directly to the Director of Finance.

A copy of the list is available in the Financial Protocol appended to these Regulations.

11.4. Credit cards etc

Credit cards, charge cards and other payment methods held in the Council's name may only be opened, closed and managed by the Director of Finance.

11.4.1. Reconciliations

Reconciliations of credit card etc accounts should be completed on at least a monthly basis by an officer who is not responsible for the processing of payment and receipt transactions through the bank accounts. The Director of Finance will ensure that reconciliations, together with supporting documentation, are reviewed and appropriately certified.

11.5. Banking arrangements

The Director of Finance will maintain an authorised signature list for Banking Transactions. The authorised signatories will be determined and approved by the Director of Finance in consultation with the Individual Cabinet Member for Finance. Authorised Signatories will normally be senior Officers who report directly to the Director of Finance.

A copy of the list is available in the Financial Protocol appended to these Regulations.

Back to Contents page

12. Taxation

12.1. Roles and responsibilities

12.1.1. Executive Directors

Executive Directors are responsible for ensuring that the VAT element of any transaction is considered with the objective of maximising VAT recovery where this is consistent with effective delivery of the service and minimising the level of irrecoverable VAT being incurred by the Council. In practice this means that they are responsible for;

- ensuring that VAT is properly accounted for on all transactions entered into by the Council,
- keeping VAT records within their area of activity , with a proper allocation of costs to exempt and other activities
- complying with all VAT legislation and regulations applicable to the delivery of their service, and
- monitoring and planning for any changes in VAT legislation or regulations which affect their areas of activity.

Executive Directors must also advise the Director of Finance of any capital projects which are under consideration which contain the risk of irrecoverable VAT being incurred by the Council, whether by way of exempt input tax or otherwise.

In circumstances where an individual, rather than a company, is engaged to provide a service to the Council, Executive Directors are responsible for ensuring that all HM Revenue and Customs regulations relating to that engagement are adhered to.

12.1.2. Director of Finance

The Director of Finance is responsible for ensuring that appropriate taxation advice is available to Executive Directors to ensure compliance with relevant legislation.

The Director of Finance is responsible for the preparation and submission of VAT Returns to H M Revenue and Customs. Such Returns are to be submitted at times which maximise the cash flow benefit to the Council, but in any event not later than the deadlines agreed with H. M. Revenue and Customs.

12.2. Penalties and charges

Portfolio budgets will bear the financial impact of any penalties or other charges imposed by H M Revenue and Customs in respect of transactions entered into by that Portfolio

.

Back to Contents page

13. Stores, Stock, Equipment and Security

Executive Directors are responsible for the care, custody and recording of stocks and equipment. This will include the following:

- Controlling access to stores etc and ensuring that stocks and assets are only used on Council business.
- Ensuring that arrangements are sufficient to ensure that additions to, as well as issues from, stock are controlled and accurately entered on the appropriate records.
- Maintaining a record of stock in hand of each item held to be physically checked at a frequency determined by Executive Directors which reflects such factors as stock values, usage etc.
- Maintaining a register of assets removed from Council premises. This includes but is not limited to assets such as laptops, mobile phones, Blackberries and RAS cards issued to officers.
- Maintaining an inventory of all assets over £100 in value, together with all attractive and portable items below this figure. The inventory should detail make, model, serial number and purchase value. Items should be recorded promptly in the inventory, at the point of purchase. The inventory should as a minimum be checked on an annual basis by physical verification of assets by an officer not involved in its compilation. A list of missing items should be provided to the Heads of Service, who will decide on the action to be taken.
- Reporting obsolete items to the relevant Head of Service for approval to write-off. Following formal, documented approval, the relevant Inventory Records should be amended accordingly.

Assets shall not be removed from the Council's premises, unless on official Council business and should not be used other than for official Council purposes or in line with arrangements sanctioned by the Council, Cabinet, an Executive Director or a Director.

All information assets such as non-public paper records, IT equipment used to access information and the computer network, must be identified, recorded and have an appointed asset owner and be appropriately protected at all times. Further details can be found in the Information Security Policy.

Some external funding regimes require specific arrangement for recording the equipment that is purchased and used to deliver the objectives of the funding. Executive Directors are responsible for ensuring that all requirements are met in this respect.

Executive Directors will provide the Director of Finance with a certificate of the stock and value held by their Portfolios at the end of each financial year as well as such information as is required in relation to stores for the accounting, costing and financial records.

Back to Contents page

14. Retention of Records

14.1. Roles and responsibilities

14.1.1. Executive Directors

Executive Directors are responsible for ensuring that all records, as defined by the Council's Document and Records Management Policy are managed in line with that Policy and that they are retained for a period that satisfies the requirements of H M Revenue and Customs, the Council's External Auditors and any other appropriate Body. The Financial Records Retention Schedule, appended to these Regulations, provides guidance on appropriate retention schedules

For any service specific records, Executive Directors are responsible for determining the retention periods with the appropriate external bodies.

Where activities, decisions or transaction are being carried out on behalf of the Council, such as in a partnership agreement, Executive Directors responsible for ensuring that appropriate records management contractual terms are in place so as to comply with the Council's Document and Records Management Policy;

14.1.2. Director of Finance

The Director of Finance is responsible for producing and maintaining a schedule on the retention periods covering financial records in accordance with current best practice. The Financial Records Retention Schedule is appended to these Regulations (Appendix C)

14.2. Records for external funding

As per Section 6 of these Regulations, all evidence required by external funding bodies must be collected and retained in line with the conditions / criteria as outlined in the funding agreement.

Where the retention period in the agreement exceeds the one prescribed in the Financial Records Retention Schedule, (see Appendix C) the funder's requirements will take precedence. As an example, ERDF requires documentation to be retained 12 years after **closure** of the Programme.

Where the retention periods required by the funder are less than those specified in the Financial Records: Recommended Retention Schedule (Appendix C of these Regulations) the latter should be followed.

Back to Contents page

15. Financial Systems

The Council's finance system is Oracle Enterprise One and this system will be the Council's prime source of accounting and financial information

15.1. Roles and responsibilities

15.1.1. Director of Finance

The Director of Finance is responsible for the Council's accounting system from which the Council's audited Accounts are produced.

The Director of Finance is responsible for controlling access to the Council's systems and information and for ensuring both the accuracy and security of the data.

The Director of Finance will ensure that the financial controls of systems interfacing with the corporate accounting system are robust and in line with the Council's information governance policies.

15.1.2. Executive Directors

Executive Directors are responsible for reconciling relevant feeder systems back to the information reported in the corporate accounting system.

Executive Directors are responsible for ensuring that Portfolio systems, e.g. CareFirst, produce financial returns in a format and to timescales required by the Director of Finance.

Executive Directors are responsible for controlling the access to Portfolio systems and information, and for ensuring both the accuracy and security of the data.

Executive Directors, in consultation with the Data Protection and Information Security Officer, are responsible for ensuring that the data held on their systems, whether held as hard copy or in electronic format, is in accordance with EU or domestic data protection legislation. Business Partners from the Business Information Systems (BIS) Team should be consulted for advice and guidance on data protection and information management issues.

Executive Directors must ensure consultation with the Director of Finance and their Business Information Systems Business Partner prior to the purchase and implementation of any new computerised financial systems. This includes any income collection systems.

Back to Contents page

16. Accounting

The Director of Finance is responsible for the form and content of the Council's Accounts and for producing the Council's Accounts for approval by the Audit Committee.

The Accounts must present a true and fair view of the financial position and transactions in respect of that financial year and be prepared in accordance with statutory requirements and all applicable professional Codes of Practice.

The Accounts will be prepared on an accruals basis.

The Accounts will be prepared on a prudent basis with income only included if it is likely to be received. Proper allowance should be made for known liabilities and losses.

16.1. Accounting during the Financial Year

All Accounts and Accounting Systems must be properly maintained throughout the year to provide timely and accurate information.

All financial transactions must be properly accounted for and adequately supported and referenced back to original documents and working papers which initiated the transaction.

Holding and Suspense Accounts must be reconciled at least monthly. Reconciliations must be produced and authorised by Officers not directly responsible for the transactions in the accounts.

Control accounts, e.g. debtors and Bank Accounts, must be reconciled on a monthly basis.

Access to accounting information will be controlled by the Director of Finance.

16.2. Year-end Requirements

At the end of each financial year the Director of Finance will produce a timetable and notes of guidance for the production of Final Accounts.

All balances on Control Accounts, e.g. Debtor Control, must be justified. Balances may only be carried forward into the next year if there is a reasonable prospect that they will be cleared.

The Accounts for the year should be "closed" at the end of business on 31 March and all income received and payments made to that date must be accounted for. The Officers responsible must certify sums held, i.e. not banked, at the close of business on 31 March.

Accruals must be supported by evidence and the Director of Finance will require copies of evidence for material accruals. The process and amounts will be specified in the year-end guidance issued by the Director of Finance.

Back to Contents page

The Officers responsible for cash floats and other cash accounts must balance and certify the amount of cash held at the close of business on 31 March.

Officers responsible for stocktaking must certify the value of stock / stores at close of business on 31 March.

Expenditure and income due for the year, but not paid or received by 31 March must be accounted for. The Officers responsible must certify the transactions concerned.

Appropriate working papers, records and prime documentation must be maintained in support of the above requirements. These will be used to substantiate the Accounts and provide a clear Audit trail.

17. Internal Audit

The Council's S151 Officer is responsible for maintaining a continuous internal audit of all the Council's financial records and operations. S /he shall be given such facilities, information and explanations as is deemed necessary to enable this to be done. Internal Audit has been provided with the authority to access any Council Officer and information necessary to carry out their duties on behalf of the Section 151 Officer.

The Charter and Terms of Reference for the Internal Audit function are contained in the Chief Internal Auditor's annual report to the Audit Committee.

An Annual Audit plan is prepared by the Chief Internal Auditor and agreed by the Audit Committee and the Council's Section 151 Officer. This is designed to cover the most significant risks faced by the Council.

As part of the audit planning process, and in line with the requirements of the Council's Risk Management Framework, Executive Directors are responsible for managing risk and for informing Internal Audit of the risks that are prevalent in their area. They are also responsible for agreeing and implementing relevant Audit recommendations.

Internal Audit report the output of its activity to the Council's Audit Committee.

17.1. Reporting potential or actual theft , fraud or corruption

Executive Directors are responsible for ensuring that they have in place adequate processes for ensuring that the Section 151 Officer is immediately notified of any circumstances indicating the possibility, or actual identification, of irregularity in funds, stores or other property of the Council. The reporting of such matters to the Council's Internal Audit Service shall be considered adequate for discharging this responsibility.

The Council's "Code of Conduct for Employees" and 'Whistleblowing Policy' as contained in Part 5 of the Council's Constitution requires any Council officer, who becomes aware of potential theft, fraud or corruption, to bring any concerns to the attention of the appropriate manager.

All employees of the Council are required to conduct themselves and carry out their duties in line with the requirements of the Code of Conduct and to comply with all Council agreed policies and procedures.

Back to Contents page

18. Companies, Joint Ventures, Partnerships, Joint Committees etc

Where the Council has a controlling interest in Companies, Joint Ventures, Partnerships, Joint Committees, or is the Lead Authority, then these organisations will be required to use the Council's finance system and to follow these regulations.

Where the Council is involved as a minority interest in partnership arrangements or Joint Committees that use their own finance systems, the arrangement must include an agreement on appropriate, robust financial governance control arrangements to the satisfaction of the Director of Finance. In these circumstances the controls in these Regulations will be used as a starting point for that agreement

No agreement shall be entered into with a Partnership which commits the Council to additional expenditure or other financial risk without approval as set out in the arrangements contained in other sections of the Regulations.

The relevant Executive Director, in conjunction with the Director of Finance will report at least annually to the appropriate portfolio holding Member and the Cabinet Member for Finance on the financial affairs of the partnership body.

19. Grant (Gift) Aid

19.1. Roles and Responsibilities

19.1.1. Director of Commercial Services

The Director of Commercial Services is responsible for ensuring there are proper processes and procedures in place for the commissioning and procurement of goods and / or services, and for the making of grant aid or 'investing' agreements.

19.1.2. Executive Directors
Executive Directors are responsible for ensuring that any Grant / Gift Aid arrangements within their area of responsibility are made in line with the Commissioning and Procurement Policy, and all other relevant processes and procedures.

Executive Directors are responsible for ensuring that all grant payments to voluntary organisations or other recipients of grant aid are properly approved in accordance with the Leader's Scheme of Delegation of Executive Functions, these Regulations and all other relevant documentation.

Executive Directors are also responsible for ensuring that the external relationship is managed in accordance with all guidance provided by the Director of Legal Services.

Back to Contents page

Appendices

A. Financial Protocol for Financial Year [2012]

A.1. Introduction

The Council’s Financial Regulations set out the high level financial rules within which all officers are required to work, without exception. More detailed Financial Policies and Procedures are available on the intranet that set out how the detailed processes underpinning these Regulations operate.

This annual Financial Protocol complements the Regulations and Policies by describing the roles and relationships of the main parties involved in the Council’s financial management arrangements. It is therefore a means to help ensure that those roles and relationships;

- ensure adherence to Financial Regulations and Policies;
- help the Council to achieve Sound Financial Management and work towards World Class standards;
- support the statutory (“section 151” – see below) duties of its Chief Finance Officer.

The Protocol will be refreshed annually by the Director of Finance for signing off with Executive Directors and Directors of Business Strategy.

A.2. Role of the Executive Director - Resources

The Executive Director of Resources will be the responsible officer (Chief Finance Officer - CFO) for the purposes of s151 of the Local Government Act 1972 and s114 of the Local Government Finance Act 1988. The Executive Director of Resources therefore has a statutory responsibility to ensure that the Council makes arrangements for the proper administration of the Council’s financial affairs. This includes ensuring the production and monitoring of these Financial Regulations. The Executive Director of Resources will recommend amendments to these Financial Regulations to the Council where she / he considers these to be in line with any changes to recommended best practice or essential service requirements or otherwise appropriate.

The Executive Director of Resources, as a member of the Council's Executive Management Team will ensure that the s151 role is discharged at this strategic level. On a day-to-day basis all s151 responsibilities may be discharged by the Director of Finance, who will act on behalf of the Executive Director of Resources in ensuring proper discharge of these statutory responsibilities. The Director of Finance is authorised to sign any and all grant claims, statutory returns or other documents that require the authority of the s151 officer on behalf of the Council. Nothing in this paragraph diminishes the ultimate financial responsibility of the Executive Director of Resources

Back to Contents page

A.3. Role of the Director of Finance

A.3.1. Statutory requirements

The Executive Director of Resources is the Council's responsible officer (Chief Financial Officer - CFO) for the purposes of s151 of the Local Government Act 1972 and s114 of the Local Government Finance Act 1988. On a day-to-day basis these duties are discharged by the Director of Finance.

The duties of the CFO can be summarised as:

- s151 – One officer shall have the responsibility to ensure that the local authority makes arrangements for the proper administration of its financial affairs.

- s114/114A - The CFO shall make a report if it appears to him / her that the Authority, a Committee, an Officer, the Executive or someone on behalf of the Executive;

    - has made, or is about to make, a decision involving the authority incurring expenditure which is unlawful,

    - has taken, or is about to take, action which if pursued would be unlawful and likely to cause loss or deficiency on part of the authority, or

    - is about to make an unlawful entry in the accounts

The CFO shall also make a report if it appears that expenditure of the authority is likely to exceed its resources.

A.3.2. Contravention of Standing Orders

In addition to the above statutory requirements, the CFO shall make a report if, in his / her view, Standing Orders have been contravened.

A.3.3. Responsibility for the Finance Service

The Director of Finance is responsible for the whole of the unified finance service within the Council. Beyond its statutory duties the Finance Service will:

- lead on the corporate financial strategy for the Council, in conjunction with the Executive Management Team,

- set clear corporate standards for "world class" financial management and ensure adherence to them,

- provide an effective business partner service to Portfolios,

- maximise efficiency and effectiveness by providing excellent shared and self service financial services,

- ensure that finance staff are confident and competent in their duties, and

- provide support and training for service managers in finance competencies.

Back to Contents page

A.3.4. Financial implications of all decisions

The financial implications of all decisions, through reports or other means, will be signed off by Finance Business Partners on behalf of the Director of Finance or directly by the Director of Finance as appropriate.

Directors of Business Strategy will also need to be involved in this process but they cannot substitute for the Finance Business Partners. The Council's Financial Regulations set out the rules for reporting financial implications.

A.3.5. Financial Returns and Grant Claims

The Director of Finance or authorised Finance Officers will sign-off all Financial Returns and Grant Claims for the Council. Details of the authorised Finance Officers are shown below and will be published alongside the Constitution as amended from time to time. The authorised Finance Officers will be responsible for signing returns / claims relating to their managerial areas of responsibility but will also authorise other returns / claims in the absence of the Director of Finance.

Deputy Director of Finance (Strategic Finance and Financial Systems Support)	Grants and returns relating to Strategic Finance and other corporate issues.
Assistant Director of Finance (Business Partner Place, External Funding and Capital)	Grants and returns relating to Place and Capital.
Assistant Director of Finance (Business Partner Communities, Revenues & Benefits and Debt Recovery)	Grants and returns relating to Communities Portfolio Revenues & Benefits and Debt Recovery
Assistant Director of Finance (Business Partner Children, Young People and Families, Resources and DCX Portfolios)	Grants and returns relating to CYPF, Resources and DCX Portfolios.

Back to Contents page

A.3.6. Documentation related to banking transactions

The Director of Finance or authorised Finance Officers will sign-off documentation related to banking transactions (see Section 11.3 of these Regulations).

Executive Director of Resources
Director of Finance
Deputy Director of Finance (Strategic Finance & Financial Systems Support)
Assistant Director of Finance (Business Partner Place, External Funding and Capital)
Assistant Director of Finance (Business Partner Communities, Revenues & Benefits and Debt Recovery)
Assistant Director of Finance (Business Partner Children, Young People and Families, Resources and DCX Portfolios)
Assistant Director of Finance (Project & Commercial)
Senior Finance Manager (Business Partner Place and External Funding)
Senior Finance Manager (Business Partner Communities)
Senior Finance Manager (Revenues and Benefits, Debt Recovery)
Senior Finance Manager (Business Partner CYPF)
Senior Finance Manager (Strategic Finance)

Back to Contents page

A.3.7. The Finance Business Partner

The Director of Finance will designate Finance Business Partner resources to provide financial advice and support to each Portfolio. The Finance Business Partners will be part of the unified finance service and their line report will be within the Director of Finance's structure. They will be held accountable for their performance to the Portfolio via the Director of Business Strategy role on behalf of the Executive Director and Portfolio Leadership Team. The ultimate responsibility for performance of the Finance Business Partner role remains with the Director of Finance.

The Director of Finance will ensure that arrangements are in place to effectively manage the relationships between Finance Business Partners and their services, Directors of Business Strategy and Executive Directors.

A.4. Role of the Executive Director:

A.4.1. Responsibility to run services within cash allocation

The Executive Director reconfirms his / her responsibility to run services within the cash allocation agreed at the special meeting of the Sheffield City Council on 9th March 2012, subject to subsequent adjustments approved within the Council's Financial Regulations, Constitution and Leader's Scheme of Delegation of Executive Functions.

A.4.2. Framework of Financial Accountability

In order to meet the statutory requirements and to protect the Council's overall financial interest the Executive Director agrees that;

- they will develop and maintain a clear, written accountability framework for the budgets held by each service and Business Unit / cost centre manager which will be linked to the sign off of this Protocol,
- arrangements are in place to ensure that the Portfolio has a clear framework for ensuring compliance with the Council's Financial Regulations and Financial Policies,
- their Director of Business Strategy will liaise with the Finance Business Partners and provide assurance annually to the Executive Director and Executive Director of Resources that the arrangements are sound;

Executive Directors are responsible for ensuring that these arrangements are working effectively, that there are proper arrangements for making managers accountable for the use of financial resources and for reviewing financial management performance.

Back to Contents page

A.4.3. Provision of financial advice to Portfolio

Finance Business Partners will act on behalf of the Director of Finance in their Portfolio and will be given the access to information and meetings that this requires.

The Finance Business Partner will be the professional financial adviser to the Portfolio and will agree the Financial Implications of all reports.

A.5. Joint Responsibilities of the Director of Finance and Executive Directors

The Executive Directors and Director of Finance will work co-operatively within the Council's Financial Regulations to ensure the effective management of the Council's financial arrangements. This will involve a commitment to influence the culture of financial management in the Council through joint working of core and business partner finance staff and the relationships between Finance Business Partners and service managers in areas such as:

- ensuring there are adequate forums for staff meetings and communications, e.g. between Finance Business Partners and Directors of Business Strategy and between Finance Business Partners and other Directors,
- training and development of finance staff and service managers to meet required financial competencies, and
- rotation and secondment of Finance Service staff to meet service needs and individual development needs.

A.6. Role of the Directors of Business Strategy

A.6.1. General responsibilities of the Directors of Business Strategy

The Director of Business Strategy (DoBS) is responsible for ensuring that:

- the Executive Director of Resources' S151 responsibilities can be discharged.
- Portfolio business is conducted in a manner that meets the highest standards of financial management, and
- the resources of the Portfolio's services are targeted at priorities and demonstrate value for money.

A.6.2. Reporting of financial issues

In relation to financial issues and implications the Director of Business Strategy is responsible for;

- making an immediate report to the Director of Finance on any financial issues of significance
- ensuring that financial implications are brought to the attention of PLT or other decision making bodies in the Portfolio, and
- ensuring that no decisions with financial implications are considered or made without being signed off by the Finance Business Partner.

Back to Contents page

A.6.3. Framework of Financial Accountability

The Director of Business Strategy is responsible for;

- developing and maintaining a framework for financial accountability with the Finance Business Partners, which will be linked to the sign off of this Protocol,
- providing annual assurance to the Executive Director and Director of Finance on the accountability frameworks for budgets and compliance with financial regulations,
- working closely with the Finance Business Partner(s) for the Portfolio to agree a more detailed protocol on roles with the Director of Finance and Finance Business Partner for key processes such as the financial strategy and budget monitoring.

A.6.4. Collaboration and Communication.

The Director of Business Strategy is responsible for ensuring that;

- the Finance Business Partner has direct access to Portfolio Leadership Teams or other meetings in the Portfolio when required,
- there are opportunities for regular liaison with the Finance Business Partners and Director of Finance,
- the Finance Business Partner or corporate shared services are the only means through which financial services and advice are provided to the Portfolio (preventing “grow back” of financial services)

A.6.5. Recruitment to post of Director of Business Strategy

The Executive Director of Resources will be involved in agreeing role descriptions and all recruitment processes to the Directors of Business Strategy posts.

Signed:

Executive Director - Resources………………………………………

Executive Director……………………………………………………

Director of Finance……………………………………………………

Director of Business Strategy

Date: .... ……………………………

Back to Contents page

B. Financial implications template v1.00 – See separate document

C. Financial Records: Recommended Retention Schedule

(Note that all figures used relate to years, e.g. Current + 6 is Current Year's records plus the previous 6 years documents)

C.1. Accountancy/Financial

General example of type of Record	Recommended Retention	Action after retention
Abstract of accounts	Current + 6	Destroy as confidential records
Annual Budget	Current + 6	Destroy as confidential records
Annual statements	Current + 6	Destroy as confidential records
Budgetary control records	Current + 6	Destroy as confidential records
Costing records	Current + 6	Destroy as confidential records
Estimate working papers	Current + 2	Destroy as confidential records
Financial ledgers	Current + 6	Destroy as confidential records
Grant claim records	Current + 6	Destroy as confidential records
Investment records	Current + 2	Destroy as confidential records
Journals	Current + 6	Destroy as confidential records
Leasing Records	Current + 2	Destroy as confidential records
Record re closing ledgers	Current + 6	Destroy as confidential records
School Fund records	Current + 6	Destroy as confidential records
Telephone call records	Current + 2	Destroy as confidential records
VAT claims	Current + 6	Destroy as confidential records
VAT records	Current + 3	Destroy as confidential records
Voluntary fund accounts	Current + 6	Destroy as confidential records

Back to Contents page

C.2. Bank related records

Type of Record	Recommended Retention	Action after retention
Bank pay-in books/slips	Current + 6	Destroy as confidential records
Bank reconciliation	Current + 6	Destroy as confidential records
Bank statements	Current + 6	Destroy as confidential records
Cancelled cheques	Current + 2	Destroy as confidential records
Cheque books and counterfoils	Current + 6	Destroy as confidential records
Cheque lists (creditors/payrolls)	Current + 2	Destroy as confidential records
Loan records and correspondence	Current + 2	Destroy as confidential records
Paid cheques	Current + 4	Destroy as confidential records
Returned cheque records	Current + 2	Destroy as confidential records

C.3. Contracts

Type of Record	Recommended Retention	Action after retention
Pre Contract Advice		
The process of calling for expressions of interest	2 years after contract let or not proceeded with	Destroy as confidential records
Specification and Contract Development		
The process involved in the development and specification of a contract	Ordinary Contract: 6 years after the terms of contract have expired. Contracts Under Seal: 12 years after the terms of the contract have expired.	Destroy as confidential records Destroy as confidential records

Back to Contents page

Type of Record	**Recommended Retention**	Action after retention
Tender Issuing and Return		
The process involved in the issuing and return of a tender (Opening Notice)	1 year after start of contract	Destroy as confidential records
Evaluation of Tender		
Successful tender document	Ordinary Contract: 6 years after the terms of contract have expired. Contracts Under Seal: 12 years after the terms of the contract have expired.	Destroy as confidential records Destroy as confidential records
Unsuccessful tender document	1 year after start of contract	Destroy as confidential records
Post Tender Negotiation		
The process in negotiation of a contract after a preferred tender is selected	1 year after the terms of contract have expired	Destroy as confidential records
Awarding of Contract		
The process of awarding contract	Ordinary Contract: 6 years after the terms of contract have expired. Contracts Under Seal: 12 years after the terms of the contract have expired.	Destroy as confidential records Destroy as confidential records
Contract Management		
Contract operation and monitoring	2 years after terms of the contract have expired.	Destroy as confidential records
Management and amendment of contract	Ordinary Contract: 6 years after the terms of contract have expired. Contracts Under Seal: 12 years after the terms of the contract have expired.	Destroy as confidential records Destroy as confidential records

C.4. Creditor records

Type of Record	Recommended Retention	Action after retention
Copy orders	Current + 2	Destroy as confidential records
Credit notes	Current + 6	Destroy as confidential records
Creditor invoices	Current + 6	Destroy as confidential records
Delivery notes	Current + 2	Destroy as confidential records
Imprest documentation (petty cash)	Current + 2	Destroy as confidential records
Period payment records	Current + 6	Destroy as confidential records

C.5. Income records

Type of Record	Recommended Retention	Action after retention
Cash books	Current + 6	Destroy as confidential records
Correspondence (income)	Current + 2	Destroy as confidential records
Debtor accounts (records non-current)	Current + 2	Destroy as confidential records
Dinner/milk registers	Current + 6	Destroy as confidential records
Income posting slips and tabulations	Current + 2	Destroy as confidential records
Periodic income records	Current + 2	Destroy as confidential records
Receipt books	Current + 2	Destroy as confidential records
Record of receipt books issued	Current + 2	Destroy as confidential records
Registrar’s quarterly returns	Current + 2	Destroy as confidential records
Sales records	Current + 2	Destroy as confidential records

Back to Contents page

C.6. Insurance records

Type of Record	Recommended Retention	Action after retention
Expired insurance contracts	Current & Permanent preservation	Destroy as confidential records
Insurance claim (fire)	Current + 4	Destroy as confidential records
Insurance claim (vehicle)	Current + 4	Destroy as confidential records
Insurance claim (public employer's liability)	Current + 6	Destroy as confidential records
Insurance policy documentation	Current & permanent	Destroy as confidential records
Insurance register	Current & permanent	Destroy as confidential records

C.7. Miscellaneous records

Type of Record	Recommended Retention	Action after retention
Capital works tabulations	Current + 2	Destroy as confidential records
Car leasing and mileage records	Current + 6	Destroy as confidential records
Car Loans	Current + 6	Destroy as confidential records
Computer system documentation	Current + 2	Destroy as confidential records
Inland Revenue docs	Current + 6	Destroy as confidential records
Internal requisitions	Current + 1	Destroy as confidential records
Inventory records	Current + 6	Destroy as confidential records
Land searches	Current + 6	Destroy as confidential records
Member allowance (statutory registers)	Current + 2	Destroy as confidential records
Minutes	Current + 2	Destroy as confidential records
Postal remittance registers	Current + 2	Destroy as confidential records
Road fund licence records	Current + 2	Destroy as confidential records
School meal records	Current + 2	Destroy as confidential records
Small holdings records	Current + 2	Destroy as confidential records
Stock lists	Current + 2	Destroy as confidential records
Travel claims	Current + 6	Destroy as confidential records
Vehicle logs	Current + 2	Destroy as confidential records

Back to Contents page

C.8. Payroll Records

Type of Record	Recommended Retention	Action after retention
BACS amendments and output	Current + 3	Destroy as confidential records
Copy payslips	Current + 6	Destroy as confidential records
Correspondence	Current + 6	Destroy as confidential records
Payroll adjustment documentation	Current + 6	Destroy as confidential records
Part – time employees' claim forms	Current + 6	Destroy as confidential records
SSP records	Current + 4	Destroy as confidential records
SSP variations	Current + 3	Destroy as confidential records
Staff transfer records	Current + 6	Destroy as confidential records
Starters forms	Current + 2	Destroy as confidential records
Tax and NI records	Current + 6	Destroy as confidential records
Tax code notifications	Current + 2	Destroy as confidential records
Timesheets and Pay Returns	Current + 6	Destroy as confidential records
Union documentation	Current + 2	Destroy as confidential records
Personnel files	Current + 2	Destroy as confidential records
Staff contracts	Current + 6	Destroy as confidential records
Unsuccessful applications	Current + 1	Destroy as confidential records

Back to Contents page

APPENDIX 3

Changes to Officers' Code of Conduct June 2012

Current	Proposed	Comment
Opening Paragraph The Code of Conduct adopted by the Governing Body will apply to employees within schools. A model 'Code of Conduct for all School Employees' and Model Procedure for the Management of the Whistleblowing Policy and Procedure for Employees in Schools are available on School point.	This Code of Conduct applies to all non school based employees. The Code of Conduct adopted by the relevant Governing Body will apply to employees within schools.	
Index Section 13 Change of Title Equality	Equality, Diversity and Inclusion	Required owing to introduction of Equality Act 2010
5 Information Technology and Data Security 5.1You must make sure you follow the Council's security procedures regarding computer use and how to treat information held on a computer. You must take care to follow these procedures when you are using passwords and logging on or off your computer. You should never share a password with anyone, because this could lead to someone without authorisation accessing the system. Sharing your password could lead to disciplinary action.	5.1 You must observe the City Council's security controls at all times. For example, non-public information held electronically is protected by passwords; you must not disclose passwords you exclusively use to access information. Written information is sometimes specially protected, for example, where disclosure is illegal. You must take care to make sure it remains protected. If you are unsure about security controls, talk to your manager or the person in charge of the information protected by them.	Required owing to introduction of Information Security Policy and deletion of Internet and Email Usage Policy and the Electronic Communications Systems Policy

5.2 You must comply with Council policies on computer use when you use the Internet or the Council intranet. These policies include the Internet and Email Usage Policy and the Electronic Communication Systems Policy. You must comply with any relevant laws when you access the Internet or intranet.	5.2 You must comply with the law and City Council policies; the Information Security Policy – which deals with security controls amongst other things. **See Appendix E** 5.3 The City Council records the use of some electronic communications use in accordance with the law. 5.4 Failure to comply with security controls or the misuse any City Council information or resources could result in disciplinary action.	Required owing to Information Security Policy being added as an appendix` and deletion of Intranet and Email Usage Policy and Electronic Communications Systems Policy
7 Secondary Employment 7.7 …Appendix E	……..Appendix F	Required owing to additional appendix under 5 above
10 Political Neutrality 10.2 ……..Appendix F	…….Appendix G	Required owing to changes in Local Government Housing Act. Removal of Scp 44 and above as criteria for being politically restricted.
10.5 If your job requires you to give advice to elected members you must keep to protocol to guide the relationship between Councillors and Officers.	10.5 If you have contact with an elected member, whether work related or of a personal nature you must keep to the council's Officer Member Protocol.	Required owing to adoption of Officer Member Protocol
11 The Local Community and Service Users 11.5 We will not accept it if any employee physically or emotionally abuses a	11.5 We will not accept it if any employee physically or	

service user, member of the public or other employee.	emotionally abuses a service user, member of the public or other employee. This includes any harassment, discrimination, victimisation or bullying.	
11.6 This includes any harassment, discrimination, victimisation or bullying.	Included in para 11.5	
11.8 We have a Dignity and Respect at Work policy. You must keep to this policy at all times.	11.6 We have an Equality and Diversity Policy. You must keep to this policy at all times.	Required owing to error in original. Original made reference in to Dignity & Respect Policy which does not apply to Service Users Equality & Diversity Policy not added as an appendix at this stage as currently under review
11.8 -12.0 renumbered		
13 Equalities	Equality, Diversity and Inclusion	
13.1 You must make sure you keep to the Council's policies on equalities. You must make sure you follow the relevant laws on equalities.	13.1 You must at all times make sure you keep to the Council's policies on equality, diversity and inclusion including behaving and working in a way which eliminates discrimination, harassment and victimisation, advances equality of opportunity and fosters good relations. See Dignity and Respect at Work Policy. **Appendix H**	Required owing to Dignity and Respect at work Policy being added to appendices

13.2 All employees and service users, elected members, partners, trade union representatives and members of the public must be treated equally and in a way that creates mutual respect. They must not be discriminated against on grounds of race, gender, disability, age, religion or sexual orientation.	All employees, customers, elected members, partners, trade union representatives and members of the public must be treated in a way that creates mutual respect. You should promote equality, diversity and inclusion by providing an environment and services free from harassment, discrimination, victimisation and bullying and by treating people with respect, regardless of their age, disability, race, religion/ belief, sex, sexual orientation or marriage/ civil partnership	
13.3 At all times employees must comply with the Council's Dignity and Respect at Work policy.	13.3 At all times you must create an environment that, promotes fairness, equality, diversity and inclusion, promotes dignity and respect for all, recognises and values individual differences and the contributions of all and actively prevents and opposes intimidation, discrimination, harassment, bullying or victimisation.	
	13.4 The Equality Act 2010 provides the legal framework for the	Required to ensure reference made to Equality Act 2010

	Council in relation to equality, diversity and inclusion.	
13.4 Breaching equality policies may be treated as misconduct, up to and including gross misconduct, which carries the possible penalty of dismissal without notice.	13.5 Breaching equality policies and the law may be treated as misconduct, up to and including gross misconduct, which carries the possible penalty of dismissal without notice.	
19.0 Date of Implementation	Insert Revised June 2012	
Glossary to Code of Conduct Equalities The Race Relations Act, Sex Discrimination Act, Disability Discrimination Act and the Employment Equality (Religion or Belief) Regulations.	**Equality Act 2010**	Required owing to introduction of Equality Act 2010

Officers’ Code of Conduct

This Code of Conduct applies to all non school based employees. The Code of Conduct adopted by the relevant Governing Body will apply to employees within schools.

Contents

1.0 INTRODUCTION

About this Code of Conduct

1.1 In the Code of Conduct, when we use the word "you" we mean a Council employee, casual worker, agency staff, contractors, volunteers, and consultants and self-employed people engaged in work for the Council.

When we use the words "we" or "us", we mean the Council.

1.2 This Code of Conduct for Employees is based on key principles. These principles are developed from the work of the Nolan Committee for standards in public life.

1.3 In the Code of Conduct you will find the minimum standards that all Council employees must keep to. These standards also apply to casual workers, agency staff, contractors, volunteers, and consultants and self-employed people engaged in work for the Council.

1.4 If you are an employee, this Code of Conduct is part of your terms and conditions of employment. Some parts of the Council may have their own Codes in addition to this one.

1.5 If your service area has its own Code, you should keep to that Code as well as this Code. You also need to follow any security policies or Codes of Practice that the council has.

1.6 We believe that you are responsible for your own actions. That means it is your responsibility to read the Code of Conduct, and any other Code which may apply to your job.

1.7 If there are any parts of this Code, or other Code, that you are unsure of or do not understand, you must ask your manager or someone in HR, to help you. This will ensure you are able to follow the Code.

1.8 You can find explanations for some of the words and phrases in this Code in the glossary section, on page 16 of this document.

1.9 This Code is not a full list of what you are expected to do or not to do. There may be other things that the Council will look at as misconduct, or gross misconduct. If there is anything that you are unsure about, please ask your manager or HR Adviser.

1.10 People who live in Sheffield expect you to have high standards of behaviour. If someone has suspicions that you could be influenced unfairly, this could damage confidence in the Council. You must not put yourself in a situation where anyone might think that you are dishonest.

1.11 The Council has the right to monitor employees. This includes surveillance. If the Council monitors employees in this way, it will keep within the laws that deal with monitoring.

1.12 You may have disciplinary action taken against you if you:

- Do not keep to this Code of Conduct.
- Commit a criminal offence.
- Do something we would classify as misconduct.
- Do something that may bring the Council into disrepute, whether during working hours or outside of them.
- Do not properly perform your duties as an employee.

Disciplinary action includes the possibility of being dismissed without notice being given.

1.13 This Code is in accordance with the rules in the Human Rights Act.

2.0 PUBLIC DUTY, PRIVATE INTEREST, FRAUD AND THEFT

(i) General

2.1 Your duty as an employee and any interests outside your job must not conflict. If there is anything you are involved in outside of work which might affect your job, you must declare this to your manager.

2.2 You must always do your job safely. To make sure you do not put the public, other employees or yourself at risk, you must follow Corporate and Directorate Health and Safety policies. You must also follow safe systems of work and any Codes of practice that apply to your job.

2.3 If you are a member of an organisation that:

- Is not open to the public
- Requires formal membership and an oath of allegiance
- Has any secrecy about its rules, the process of becoming a member, or conduct of members.

2.4 You must declare this in writing to your Head of Service or Director. For further information on what we call a secret society, read **Appendix A.**

2.5 The Council has responsibility for the administration of public money. We emphasise to the public and to employees that we think honesty and that having proper control of finances is very important.

2.6 The Council is committed to the fight against fraud, whether an employee, a contractor, or a member of the public has committed the fraud.

2.7 You must not use the fact that you are a Council employee to obtain, gain directly or indirectly - for yourself, any business associates, your friends or your family.

2.8 As the Council is committed to the prevention and detection of fraud, we have a policy statement on Fraud and Corruption. This is shown in **Appendix B**.

2.9 We also have a Gifts and Hospitality Policy and Code of Practice. This is shown in **Appendix C**.

2.10 In addition to these two policies, we have a Whistleblowing Policy and Procedure, so that you can report any fraud or corruption more easily. This is shown in **Appendix D**.

2.11 If you are using public funds, you must use them responsibly, and you must keep within the law. You must make sure that we use our resources sensibly and legally, and that the community gets value for money.

2.12 You must keep to the rules within the Council's Standing Orders and Financial Framework. The Standing Orders are available on the Council's Internet site.

2.13 If you:

- Commit fraud against the Council, or any person or organisation, or try to.
- Steal from the Council, or any person or organisation, or try to.

2.14 This will be considered misconduct and may be considered gross misconduct. This includes deliberately putting false information on time sheets, subsistence claims or mileage claims.

2.15 If you have concerns that someone is stealing, committing fraud or behaving in a way that might be unethical, you must report this to your manager, or someone named in the Whistleblowing Policy and Procedure. This procedure is shown in **Appendix D**.

2.16 We know that it is not always easy to report on the behaviour of other people. We will give you full support if you raise concerns. If you wish to remain anonymous, we will make every effort to respect this.

2.17 We know there are two sides to a story, and we will ensure hearings are fair.

2.18 Sometimes allegations will turn out to be wrong. If you deliberately make false or malicious allegations, this will be treated as misconduct.

(ii) Financial Inducements, Gifts and Hospitality

2.19 You must never accept a financial payment, bribes or inducement from any individual, body, or organisation. For example: payments or inducements from contractors, developers, or consultants.

2.20 To take financial payments or inducements is against the law. It is an offence under Section 117 of the Local Government Act 1972.

2.21 You must refuse any gift or hospitality offered to you or your family that others may think could influence you.

2.22 You may accept gifts of small value such as pens, diaries and calendars.

2.23 For further guidance on gifts, hospitality and inducements, you can read the Gifts and Hospitality Policy and Code of Practice. This is shown in **Appendix C**.

2.24 Any gifts or hospitality you have been offered, whether you have turned them down or accepted them, must be recorded. If you are unsure of the process of recording goods and hospitality in your service area, seek advice from your manager.

(iii) Employee Declarations of Financial and other interests

2.25 You have a legal duty to declare any financial or other interest in an existing or proposed contract.

2.26 You have a legal duty to declare any interest in or associations that may cause direct or indirect conflict with your work for the Council. You must declare interests in or associations with any:

- Organisation
- Service
- Activity
- Person

2.27 If the Council has sponsored an event or a service, you must tell your Head of Service or Director if you may benefit from it in any way.

2.28 You must also tell your Head of Service or Director if anyone connected with you will benefit from it. This includes your relatives, your partner or spouse, or any business associates you may have.

2.29 You must fully explain any way you or someone connected with you may benefit.

2.30 If the Council gives support in the community, through financial help or other help, you must make sure that any advice you give is fair and balanced. You must make sure that there is no conflict of interest.

2.31 If you apply for a service that you have influence in because of your job, you must declare a personal interest, both when you apply for the service, and to your manager.

2.32 You must also declare a personal interest if you help someone you know from outside your job to apply for a service you have influence in.

2.33 You are free to use all Council services. If you do so, you will not be treated more or less fairly because you work for the Council.

2.34 Members of the public expect you to be fair and treat people equally, no matter who you are delivering services to.

2.35 You must make sure you don’t do anything in your job that might make people think you are being unfair or biased.

2.36 You must not try and obtain services in a different way to the public because you work for the Council. This includes putting pressure on colleagues to get services.

2.37 If you think there might be a conflict of interest, you must look at any procedures that are in your Portfolio to find out what to do. If you are not sure, you should ask your manager to help you.

2.38 The Monitoring Officer will review any declarations that have been made every year. If the Monitoring Officer needs to make declarations, the Chief Executive will review them every year.

2.39 The Director of Human Resources is responsible for making sure all the Employment Policies, Practices and Procedures that the Council has are kept to.

2.40 Every Head of Service, Director and Executive Director is responsible for monitoring their employees activities, making sure they have kept to this Code and any other Codes and made declarations when they need to. Any monitoring will comply with all relevant laws.

3.0 CONTRACTORS

3.1 As part of your job, you may be required to supervise or engage contractors or have an official relationship with them. If you have any work relationship with contractors, or potential contractors, you must tell your Head of Service or Director in writing if you have ever had a private or domestic relationship with the contractors.

3.2 The orders we place and contracts we give should be given fairly. This means that we must award orders and contracts based on merit and fair competition against other tenders. You must not show favouritism in doing this. For example, if your friends, partners or relatives run a business, you could not award them a contract unfairly because of this. You must not discriminate against anyone unfairly if you deal with tenders, evaluation or awarding contracts.

4.0 RELATIONSHIPS WITH PROSPECTIVE AND CURRENT CONTRACTORS

4.1 If you are involved in the process of tendering and dealing with contractors you should understand that being a client and being a contractor are two separate roles. If you have a client or contractor responsibility, you need to be open and accountable for your actions.

4.2 If you work in a contractor or client unit you must be fair and impartial when you deal with customers, suppliers and any other contractors or subcontractors.

4.3 If you have access to any information about contracts or costs for contracts that is not public, you must not disclose that information to anyone unauthorised.

4.4 You must make sure that you don't show special favour to anyone who works for us or used to work for us when you award contracts. You must make sure you do not show special favour to anyone who is a partner, associate or relative of an employee when you award contracts.

4.5 If you are thinking about a 'management buyout', you must inform the Chief Executive as soon as you definitely intend to do it. You must also inform your Executive Director and Head of Service or Director. You must withdraw from doing any work for us that includes preparation, tendering, evaluation, and awarding contracts or orders.

4.6 If Competitive tendering is being carried out, and you are involved in the process, you must let your Head of Service or Director know when you are a member of an organisation that is interested in tendering. You must also let your Head of Service or Director know if you have affiliation to an organisation that is interested in tendering.

5.0 INFORMATION TECHNOLOGY AND DATA SECURITY

5.1 You must observe the City Council's security controls at all times. For example, non-public information held electronically is protected by passwords; you must not disclose passwords you exclusively use to access information. Written information is sometimes specially protected, for example, where disclosure is illegal. You must take care to make sure it remains protected. If you are unsure about security controls, talk to your manager or the person in charge of the information protected by them.

5.2 You must comply with the law and City Council policies; the Information Security Policy – which deals with security controls amongst other things. **See Appendix E**

5.3 The City Council records the use of some electronic communication use in accordance with the law.

5.4 Failure to comply with security controls or the misuse any City Council information or resources could result in disciplinary action.

6.0 USE OF COUNCIL SYSTEMS, PROPERTY AND FACILITIES

6.1 Anything that belongs to the Council, including:

- Telephones- including mobile phones
- Computers- including laptops
- Stationery
- Offices
- Car parks
- Vehicles
- Facilities

can only be used for Council business unless permission is given by management.

6.2 If, with your managers' permission, you use a Council telephone or mobile telephone to make private calls or text messages, or send private faxes using a Council fax machine, you must pay for this through the approved systems in place. If you are unsure about how to pay for calls, speak to your manager.

6.3 The Council has systems in place that log telephone, email and Internet usage. These systems may be used to identify any usage for private purposes. We may monitor any communications using Council systems. If we monitor your use of Council resources, we will do it within the law and Council policy.

6.4 You must keep to any Council system security measures.

7.0 SECONDARY EMPLOYMENT

7.1 We prefer you not to have other paid employment whilst you are working with the Council. This includes paid work for another employer and working in a self-employed or business partnership basis.

7.2 If you do have any other employment whilst you are working for the Council, the work you do must not conflict with the interests of the Council or bring it into disrepute. You must only do other work outside of your working hours with the Council. You need the formal prior permission of your manager to do any work outside your role with the Council.

7.3 We particularly ask that you do not use any professional skills that you use in the course of your employment to do paid work for someone else within the Authority area.

7.4 If you do any work that is damaging to the interests or reputation of the Council, we may take disciplinary action against you, even if you have declared this work to your manager.

7.5 If you are a:

- School Governor
- Councillor for another Local Authority
- Member of the Territorial Army
- Justice of the Peace
- Member of an Employment Tribunal

7.6 These roles do not count as Secondary Employment. You should still make your manager aware of these duties and ask for any time off you need in a reasonable and timely manner. Unpaid voluntary work in the Community is not secondary employment, but you still need to declare it to your manager, as there may be a conflict of interest with your Council job.

7.7 You can find further guidance on receiving payment or fees for other work in **Appendix F**.

8.0 DISCLOSURE OF INFORMATION, CONFIDENTIALITY AND REFERENCES

8.1 You should be fair and open when you deal with others. You should make sure that elected members and members of the public have access to information they need unless there is a good reason not to allow this, according to the Freedom of Information Act.

8.2 You must act in accordance with the law when handling personal and other information. You must take special care when handling personal and confidential information, and never use it inappropriately. You may be prosecuted personally under the Data Protection Act, so it is important you know what your responsibilities are. If you are unsure about this, consult your manager. The Council also has a Data Protection and Security Officer who can help.

8.3 You must not disclose any confidential, personal or financial information about an employee to an unauthorised person. You must not disclose any personal or financial information about an employee to any external agency without their approval. If you are not sure who is an authorised person, you should consult the Director of Human Resources.

8.4 If you are asked for personal information for a reference, for example for a job or mortgage application, you may provide information only after you confirm the identity of the enquirer. To do this, you can reply in writing to the enquirer, or call them back to make sure they are who they say they are.

8.5 If the request is for a reference for a colleague or ex-employee, only the employee's line manager can provide an employment reference. Any employee may give a reference in a personal capacity. If you misrepresent the Council, this will be treated as misconduct.

8.6 You must not disclose confidential information to a third party. This includes information relating to:

- Competitive tendering or tendering for work.
- Exempt items under the Local Government (Access to Information Act, 1985)
- An employee, elected member or service user.

8.7 You must not use any information that you get in the course of your employment for personal gain, or give it to anyone else who may use it in this way.

8.8 If in the course of your job, you deal with someone you're related to, or have a close relationship with, declare it to your manager. You must be fair and act in a professional way.

8.9 Inappropriate disclosure of confidential information can be considered misconduct, and may be considered gross misconduct which can lead to dismissal.

9.0 COMMUNICATIONS WITH THE MEDIA

9.1 All contact with the media that is about Council activities is handled by the Communications service, together with Heads of Service, Directors and Executive Directors. If you have an idea for a positive story about something the Council is doing, or if a journalist approaches you, you must contact the Communications Service to get approval before you give any information. This includes giving information verbally, through e-mail or in writing.

9.2 If you are writing something that will be published, and it doesn't talk about the Council but does relate to your job, you should tell your Head of Service or Director before it is published. An example of this might be an article in a professional journal.

10.0 POLITICAL NEUTRALITY

10.1 You must not allow your personal or political opinions to interfere with your work. Some posts are "politically restricted". If this applies to you, you should already have been told about the restrictions separately.

10.2 More information on this is available in **Appendix G**. If you need any more advice or information, ask your manager or HR Adviser.

10.3 You work to all elected members and must ensure their rights are respected. You must not be biased in dealing with members of one political group rather than another.

10.4 If your job requires you to advise political groups, you must make sure you take a neutral stance and point of view.

10.5 If you have contact with an elected member, whether work related or of a personal nature, you must keep to the Protocol for Member Officer Relations.

10.6 If you are on Council business, you must not wear anything that shows you are in favour of or against a political party or a pressure group. You may not display any items showing political affiliation or opposition on your vehicle, or items like tools or other equipment.

11.0 THE LOCAL COMMUNITY AND SERVICE USERS

11.1 You must remember that you have a responsibility to people in Sheffield. You must make sure that you deliver services politely, efficiently and fairly to everyone in the community.

11.2 You should be as open as possible about what you do, and the work of the Council.

11.3 You must not do anything that might affect confidence in the Council.

11.4 You should make sure that you keep to the law and any other guidance.

11.5 We will not accept it if any employee physically or emotionally abuses a service user, member of the public or other employee. This includes any harassment, discrimination, victimisation or bullying.

11.6 We have an Equality and Diversity Policy. You must keep to this policy at all times.

11.7 If you act in this way it may be decided that is misconduct or gross misconduct, which can result in disciplinary action including dismissal.

11.8 When you work with young people or vulnerable adults you are in a position of trust. If you abuse that trust, it will be regarded as potential gross misconduct.

11.9 Any sexual misconduct or assault will be regarded as potential gross misconduct.

11.10 If you do not follow any policies or procedures meant to keep vulnerable service users or others safe, this will be regarded as potential gross misconduct.

11.11 Any act of gross misconduct may lead to disciplinary action and the possibility of dismissal without notice.

11.12 If you work with young people or vulnerable adults, you must read any relevant Codes of practice as well as this Code, and keep to them. You must keep to any relevant laws, such as the Children's Act and the Child Protection and Adult Abuse Protection Procedures.

11.13 If you see any abusive behaviour, you must report it to your line manager, or use the Whistleblowing policy (see **Appendix D**) to report it.

12.0 RECRUITMENT AND OTHER EMPLOYMENT MATTERS

12.1 If you are involved in recruitment, you must take care not to discriminate against anyone, or in favour of anyone. You must keep to the Recruitment and Selection Code of Practice in full.

12.2 To make sure you are not acting unfairly, you must not be involved in any selection and appointment (for example, interviewing someone) when you are related to an applicant. You must not be involved in selection or appointment where you have a close relationship with an applicant- personal or business.

12.3 If you think there might be a conflict of interest, you must inform your manager or HR Adviser.

12.4 Decisions that you make at work should be fair and unbiased. You must not be involved with decisions to do with discipline, promotion, or pay for anyone who is related to you, or someone you have a close relationship with. This includes personal relationships and business relationships.

12.5 If there are any reasons why 12.1-12.4 should not be followed, or you need help and advice with what to do next, you should contact the Director of Human Resources.

13.0 EQUALITIES

13.1 You must at all times make sure you keep to the Council's policies on equality, diversity and inclusion including behaving and working in a way which eliminates discrimination, harassment and victimisation, advances equality of opportunity and fosters good relations. See Dignity and Respect at Work Policy. **Appendix H**

13.2 All employees, customers, elected members, partners, trade union representatives, and members of the public must be treated in a way that creates mutual respect. You should promote equality, diversity and inclusion by providing an environment and services free from harassment, discrimination, victimisation and bullying and by treating people with respect, regardless of their age, disability, race, religion/ belief, sex, sexual orientation or marriage/civil partnership.

13.3 At all times you must create an environment that, promotes fairness, equality, diversity and inclusion, promotes dignity and respect for all, recognises and values individual differences and the contributions of all and actively prevents and opposes intimidation, discrimination, harassment, bullying or victimisation.

13.4 The Equality Act 2010 provides the legal framework for the Council in relation to equality, diversity and inclusion.

13.5 Breaching equality policies and the law may be treated as misconduct, up to and including gross misconduct, which carries the possible penalty of dismissal without notice.

14.0 DRESS AND PERSONAL APPEARANCE

14.1 When you work for the Council, you are a representative of your service, and of the Council. You must dress in a way that is appropriate, or required, for your workplace and the work you are doing. You must be clean and tidy and make sure you have good personal hygiene.

14.2 If you are provided with clothing for uniform or health and safety reasons, you must wear it. This includes your name badge and other identity badges where provided.

15.0 HEALTH AND SAFETY

15.1 You have a responsibility to work safely and make sure your working environment is healthy and safe. You are required to keep to Corporate Health and Safety Policies. You are also required to follow any policy, regulations or Codes of practice on Health and Safety that apply to your Portfolio or area of work.

15.2 You must keep to any relevant Health and Safety laws.

16.0 CRIMINAL CONVICTIONS

16.1 If your job is covered by the Rehabilitation of Offenders Act, you must tell us about all convictions, including “spent” convictions, before you start working with us. You must tell us about any convictions where the Exemptions orders to this Act apply.

16.2 If you do not tell us about these convictions this will be treated as possible gross misconduct and might lead to disciplinary action - including the possibility of dismissal without notice.

16.3 If your work involves driving, you must tell your manager about any driving offences, or pending driving offences.

16.4 If you work with young people or vulnerable adults as part of your job, of if you have access to them; you must report any convictions that you have, whatever they are, to your manager.

16.5 You must tell your manager if you have any criminal proceedings pending against you.

16.6 If you work with young people or vulnerable adults and you believe that you are or might be thought of as a risk to these groups it is extremely important that you seek advice from your manager. If you do not disclose this, this can be treated as misconduct, including gross misconduct which carries a possible penalty of dismissal.

17.0 DRUGS AND ALCOHOL

17.1 While you are at work, you must be in a condition to do your job safely.

17.2 The effects of drinking alcohol cause you to perform your work less well. It may also be a health and safety risk- especially if you drive or use machinery. Because of this, you must not drink alcohol:

- Before you start work
- During your working hours
- During a lunch break from work
- On any other break during your working day
- At functions such as conferences within working hours.

17.3 If you drink alcoholic drinks at these times, this may be regarded as misconduct or gross misconduct, which could lead to dismissal.

17.4 If you use illegal drugs, or prescription drugs that have not been prescribed for you, this will not be accepted. This may result in the Council contacting the police to report it. Use of illegal drugs or prescription drugs that have not been prescribed for you before or during work, on breaks or at functions may be considered misconduct or gross misconduct, which could lead to dismissal.

18.0 GENERAL CONDUCT

18.1 You must follow instructions, providing they are lawful. You must make sure you do not do anything that might affect the Council's legal position. You should show respect for service users, colleagues and elected members.

18.2 We expect you to use good judgement, and take account of other people's views. We expect you to take responsibility and decide your own view on any issue that comes up while you work for the Council.

18.3 If you need further information or advice about what to do in a situation, you should contact your manager, an HR Adviser or the Chief Internal Auditor.

18.4 You should read this Code together with the appendices, and any other Codes of Practice or policies that are about conduct or security.

19.0 DATE OF IMPLEMENTATION

Revised June 2012

20.0 APPENDICIES

A Definition of what constitutes a membership of Secret Society

B Policy statement on Fraud and Corruption

C Gifts and Hospitality Corporate Policy and Code of Practice

D Whistleblowing Policy and Procedure

E Information Security Policy

F Other employment related to activities – fees

G Politically Restricted Posts

H Dignity and Respect at Work Policy

GLOSSARY TO CODE OF CONDUCT

Contractor- An individual, partnership, company or other service that has a contract with us to do or provide something. For example, to design, develop, manufacture, maintain or provide services.

Conflict of Interest- A conflict between private interests and your duties with the Council. This can exist whether or not money is involved, and whether the conflict is actual or just perceived.

Competitive Tender- Where several potential contractors are invited to prepare proposals to provide a project or service, on the basis of quality and price.

Disciplinary- Disciplinary action is action taken by an employer for violating policy or procedure (including the Code of Conduct). For more details on this, see the Council’s Disciplinary Policy.

Disrepute- To bring something into disrepute is to lower its reputation, damage its image.

Misconduct- Breaking the Code of Conduct, another Code or terms and conditions may be considered misconduct. There are different types of misconduct depending on the exact circumstances and consequences. The most serious type is **gross misconduct**. For more information on this, see the Council’s **Disciplinary Policy**.

Inducement- something that encourages you towards an action- an incentive. This could be money, food, gifts, or anything else that might benefit you. If you are offered or take something that people may think is an inducement, you could be accused of making decisions unfairly based on what you received.

Whistleblowing (also ‘whistle blowing’)- Revealing wrongdoing to someone in authority. For more information on this, see **Appendix D,** the Whistleblowing policy.

RELEVANT LAW

This section points to relevant law on some topics from the Code of Conduct. It should not be considered an exhaustive list as legislation frequently changes. If you are unsure about whether an action would be lawful, please investigate further.

Monitoring and Surveillance:
The Regulatory and Investigatory Powers Act, the Data Protection Act, and the Human Rights Act.

Use of IT Equipment:
The Data Protection Act, The Obscene Publications Act,
The Computer Misuse Act, The Theft Act.

Equalities:
Equality Act 2010

APPENDIX A

DEFINITION OF WHAT CONSTITUTES A MEMBERSHIP OF SECRET SOCIETY

The following is the Council's definition of what constitutes a society with secret rules (secret society).

'Any lodge, chapter, society, trust or regular gathering or meeting, which:

a) **is not open to members of the public who are not members of that lodge, chapter, society or trust; and**

b) **includes in the grant of membership an obligation on the part of the member a requirement to make a commitment (whether by oath or otherwise) of allegiance to the lodge, chapter, society, gathering or meeting; and**

c) **includes, whether initially or subsequently, a commitment (whether by oath or otherwise) of secrecy about the rules, membership or conduct of the lodge, chapter, society, trust, gathering or meeting.**

A lodge, chapter, society, trust, gathering or meeting as defined above should not be regarded as a secret society if it forms part of the activity of a generally recognised religion.

APPENDIX B

Article I.

Article II. Policy Statement

Article III. Fraud & Corruption

Contents

Section 3.01

1. Statement from the Chief Executive

Sheffield City Council, like all other local authorities, is charged with the responsibility of protecting the public purse and ensuring that its resources are utilised in the best possible manner to serve the community.

One of the key priorities of our Corporate Plan is ‘Effective Resource Management’ and one of its guiding principles is to achieve ‘Value for Money’. This is why the Council is committed to a zero tolerance environment in relation to fraud and corruption.

The public is entitled to demand the highest standard of conduct from our employees and members and it is essential that we are able to demonstrate this and maintain public faith. Every pound lost to fraud or misappropriation is a pound which cannot be invested in our services.

We are committed to the prevention, detection and investigation of potential fraud and corruption and, where proven, we will seek the strongest appropriate sanctions against those responsible.

It is the duty of each of us, as members and employees of the Council, to maintain standards as detailed in Codes of Conduct and to report any suspicions of fraud through appropriate channels.

John Mothersole
Chief Executive
(Signature)

2. Introduction

This document sets out Sheffield City Council's policy and strategy in relation to fraud and corruption. It has the full support of the Council's Members and the Executive Management Team.

The Council is committed to sound corporate governance and supports the Nolan Committee's 'Seven Principles of Public Life' for the conduct of Council Members and Employees; namely: -

- **Selflessness** – Making decisions based solely upon the public interest
- **Integrity** – Not engaging in financial or other obligations with external parties which may influence decision making in the workplace
- **Objectivity** – Making work-related choices solely on merit
- **Accountability** – Exposing one's actions and decisions to an appropriate level of public scrutiny to demonstrate their propriety
- **Openness** – The ability to justify decision making via logical argument. Only restricting information if wider public interest demands this course of action
- **Honesty** – Declaration of private interests and addressing conflicts to protect the public interest
- **Leadership** – Promotion of the above principles by example

In order to most effectively deliver the Corporate Plan, we need to maximise the financial resources available to us. To achieve this, we must reduce fraud and misappropriation to an absolute minimum.

Our strategy aims to achieve a strong Council wide anti-fraud ethos in an environment which promotes intolerance of fraud and corruption and which provides full support and protection to those who speak out against it.

We will achieve this via the establishment and maintenance of an internal control structure which incorporates and effectively mitigates the risks associated with fraud and corruption. This will be complemented by clear policies and procedures which focus on: deterrence, prevention, detection, investigation, sanctions and redress.

We will actively promote this strategy across the authority.

3. Definition of Fraud & Corruption

The Fraud Act 2006 breaks the offence of fraud into 3 distinct categories as follows:

- "Fraud by false representation" is defined by Section 2 of the Act as a case where a person makes "any representation as to fact or law ... express or implied" which they know to be untrue or misleading.

(Example: The submission of a timesheet for an employee which records more hours than those actually worked.)

- "Fraud by failing to disclose information" is defined by Section 3 of the Act as a case where a person fails to disclose any information to a third party when they are under a legal duty to disclose such information.

(Example: A benefit claimant whose circumstances change meaning that they are no longer entitled to benefit, fails to inform the Authority of this change of circumstances.)

- "Fraud by abuse of position" is defined by Section 4 of the Act as a case where a person occupies a position where they are expected to safeguard the financial interests of another person, and abuses that position (this includes cases where the abuse consisted of an omission, where there is a legal requirement to disclose, rather than an overt act.)

(Example: A care worker claims to have spent monies belonging to a service user on items for the benefit of that person but has actually taken the monies for him/herself.)

In all three classes of fraud, for an offence to have occurred, the person must have acted dishonestly, with the intent of making a gain for themselves or anyone else, or inflicting a loss (or a risk of loss) on another.

Corruption is defined as: The act of offering, giving, soliciting or accepting an inducement or reward, which may influence the action of any person. Although similar to the third offence of the Fraud Act, corruption by definition indicates the involvement of a third party.

For clarity and for the purpose of this policy, ‘internal fraud’ can be characterised as: Council employees or members, either alone or in collusion with other parties, attempting to misappropriate funds, stores, equipment or other council assets and attempting to hide such activity via the modification, manipulation or destruction of council records.

‘External fraud’ can be defined as: A third party individual, company or other organisation attempting to obtain council grants, loans, benefits or other funds, property or assets to which they are not legally entitled, via deception, misrepresentation, failure to disclose information or other dishonest method.

4. Fraud indicators

Those who commit fraud do so for a particular reason. This may relate to financial hardship, greed, opportunity or a perceived lack of deterrent or sanction. Whatever the motive, there are often indications, which are observable by colleagues and / or managers, that fraud may be taking place. Members and employees should be aware of typical indicators to improve the likelihood of identifying existing fraud and corruption. A non exhaustive list of fraud indicators is detailed below:

- Employees who appear to be under stress without a high workload.
- People who are consistently first to arrive in the morning and last to leave at night.
- A general reluctance to take leave for any significant period.
- Refusal of promotion.
- Unexplained wealth or claims of ‘independent means’.
- A sudden change of lifestyle including large individual purchases.
- ‘Cosy’ relationships with suppliers / contractors.
- Suppliers / contractors / clients who insist on dealing with one particular member of staff.
- Known to be in serious financial difficulty.

In addition to the above generic indicators, employees / members should consider other fraud indicators, including those relating to ‘external fraud’ against the authority, which are specific to their service area.

It should be noted that the existence of one or more of these indicators is not proof that inappropriate activity is taking place. **They are merely ‘warning signs’** which may give cause for managers to more closely review the activities of certain employees.

Further information relating to fraud indicators and fraud risk management may be found on the intranet: Risk Management

5. Employees’ / Members’ Responsibilities

Employees of the Council are required to follow the Council’s Code of Conduct and report to management instances of outside interests, gifts and hospitality. Under the City Council’s Standing Orders, employees must operate within legislative requirements which include Section 117 of the Local Government Act 1972. Section 117 requires the disclosure of pecuniary interests in contracts relating to the City Council, or the acceptance of any fees or rewards whatsoever other than their proper remuneration.

Members are expected to operate honestly and without bias. Their conduct is governed by:

- National Code of Local Government Conduct.

- Sections 94-96 of the Local Government Act 1972.
- Local Authorities Members' Allowances Regulations 1991.
- City Council Standing Orders.

These matters are specifically brought to the attention of Members at the Induction Course for New Members and are in the Members' pack of information issued by Legal & Governance. They include rules on the declaration and registration of potential areas of conflict between Members' City Council duties and responsibilities, and any other areas of their personal or professional lives.

> "Defrauding and stealing (or attempting to do so) from the Council or any person or organisation in any way will not be tolerated"
>
> "The Council **requires** its employees to report genuine concerns relating to potential fraud, theft or unethical behaviour"
>
> *Officers' Code of Conduct*

6. Contractors & Partners

Organisations providing services on behalf of Sheffield City Council are expected to maintain strong in-house counter fraud procedures. Employees of partner / contractor organisations are required to abide by the principles of this policy statement. The council will incorporate such requirements into partnership contracts and will reserve the right to inspect any pertinent company documentation in the case that fraud is suspected. Major partners will be expected to maintain an effective fraud policy and have publicised internal arrangements for whistleblowing.

7. Counter Fraud Activities

(a) Deterrence

It is preferable that 'would-be fraudsters' are deterred from conducting fraudulent activities within the Council environment. Deterrence negates the requirement for time-consuming and costly investigations where fraud has already occurred. However, where fraud has occurred and is proven, Sheffield City Council is committed to exposing fraudsters and seeking the strongest and most appropriate sanctions available.

Acts of theft, fraud or corruption by Sheffield City Council employees will be regarded as Gross Misconduct. Where this is proven, such acts will result in dismissal. Additionally, it is Council policy to seek criminal prosecution in cases of fraud committed against the Authority.

Where circumstances permit, we will publicise the details of fraudsters in co-operation with appropriate media and furthermore will share information with other organisations to prevent fraudsters from obtaining positions of trust elsewhere. We will respect and abide by the principles of the Data Protection Act in relation to the sharing of information.

(b) Prevention

The Council recognises that a key preventative measure in the fight against fraud and corruption is to take effective steps in the recruitment stage to establish, as far as possible, the propriety and integrity of potential staff.

To this end, Directors / Heads of Service are required to ensure that suitable references are obtained before employment offers are confirmed. This requirement applies to the employment of permanent, temporary and contract employees.

Council Management has established a system of internal controls across the whole network of financial, operational and managerial systems to ensure that its objectives are achieved in the most economic and efficient manner. Incorporated into these are controls specifically designed to prevent and / or detect fraudulent activities. In order to most effectively minimise the risk of fraud, managers should ensure consistent compliance with internal control processes.

Heads of Service are required to formally acknowledge that fraud risks have been identified and effectively mitigated within their service area. These declarations form part of the Annual Governance Statement for the Authority.

The Financial Regulations of the Council provide the framework for financial control. Under Financial Regulations: -

- Each Executive Director will be responsible for ensuring the proper financial management of their Directorate services and compliance with the Financial Regulations by staff within their Directorate.

The Council's internal audit service independently monitors the existence, appropriateness and effectiveness of internal controls.

(c) Detection

Financial Regulations state that: -

- The Director of Corporate Resources and Director of Finance shall be notified by Executive Directors immediately any circumstances indicating the possibility of irregularity in cash, stores or other property of the Council are discovered*. The Council's "Code of Conduct for Employees" and 'Whistleblowing Policy' requires any Council officer, who becomes aware of potential theft, fraud or corruption, to bring any concerns to the attention of the appropriate manager. All employees of the Council are required to conduct themselves and carry out their duties in line with the requirements of the Code of Conduct.

*In practice, Internal Audit acts on behalf of the Director of Corporate Resources / Director of Finance in this area and allegations should normally be directed to the Chief Internal Auditor.

Employees / Members who suspect or become aware of theft, fraud or corruption should refer to the whistleblowing policy on the Council's Intranet. The Council is committed to the principles of the Public Information Disclosure Act which assures that persons who speak out about wrongdoing are protected, providing their disclosure is made in good faith

Fraud has been identified as an inherent risk within the Council's activities and has been incorporated into its risk management strategy accordingly.

Operational audit programmes include testing to assess the effectiveness of internal control procedures. Where these processes are found to be inadequate, probity testing is undertaken to identify whether control weaknesses have been exploited and fraud or theft has occurred.

The Council operates a pro-active approach to fraud detection utilising all methods available including: data matching, open source research, targeted probity exercises, surveillance and intelligence-led investigation. It also actively participates in the Audit Commission's National Fraud Initiative (NFI).

(d) Investigation

Allegations of fraud or corruption will be investigated in a timely and professional manner to protect the interests of both the Council and the individual(s) implicated. An allegation or suspicion will not be viewed as proof of guilt and investigators will conduct investigations fairly and with an unbiased approach. In investigations where interviews under caution are appropriate, these will be conducted by suitably trained officers in accordance with the requirements of the Police and Criminal Evidence Act.

(e) Recovery

Where fraud or misappropriation has taken place, the Council will use the full range of methods at its disposal in order to recover monies / assets. Such recoveries will be returned to the appropriate stakeholder.

(f) Third Party Liaison

Sheffield City Council acknowledges that in order to fight fraud and corruption it cannot afford to work in isolation. Consequently it has fostered active liaison arrangements with a number of external bodies. The aim of these arrangements is to maximise the effectiveness of counter fraud and corruption activities via the exchange of intelligence, expertise and experience.

Currently, arrangements exist with the organisations below; however, the Council will continue to seek beneficial relationships with other organisations for continual improvement in this area:

- South Yorkshire Police
- South and West Yorkshire Investigators Group
- Core City Chief Internal Auditors
- Audit Commission
- The Department for Work & Pensions (DWP)
- National Anti-Fraud Network (NAFN)
- Local Authority Investigation Officers Group (LAIOG)
- Capita

8. Summary

The Council recognises that the vast majority of its Employees and Members have high standards of personal and professional integrity and carry out their duties to the best of their ability in order to provide a high quality service to the citizens of Sheffield.

However, despite our efforts, there will be individuals who will seek to exploit their knowledge or position in order to achieve personal gain. Fraud involving public monies is justified in the minds of fraudsters as a ‘victimless crime’. This is far from the truth. As guardians of public funds, it is essential that Council Members and employees work together to ensure that these funds are protected and put to their intended use.

Further information relating to matters contained in this policy can be found in the Internal Audit section of the Council’s intranet site: Internal Audit - Fraud / Whistleblowing

APPENDIX C

GIFTS AND HOSPITALITY

CORPORATE POLICY AND CODE OF PRACTICE

Article IV. The purpose of this document is to clearly inform employees of the policy and procedure in relation to offers of gifts and hospitality made from any source.

1. Policy

1.1 The City Council's Code of Conduct states that the public is entitled to demand of a local government employee conduct of the highest standard. Employees' actions must not be influenced by offers of gifts or hospitality and their actions must not give the impression that they have been influenced in this way.

1.2 Council employees must not accept gifts, loans, fees or rewards from any person or organisation in particular those who may potentially expect to receive an advantage or benefit in return. This includes gifts, loans, fees or rewards from contractors, outside suppliers or members of the public. However, some incidental gifts or hospitality can be accepted, as detailed in this Code of Practice.

1.3 This Code of Practice applies to all employees of the City Council, including Executive Directors and the Chief Executive.

1.4 Any breach of this Code of Practice may be viewed as potential gross misconduct and could lead to a disciplinary hearing that may result in summary dismissal.

2. Principles

2.1 Employees must maintain a good working relationship with the public but avoid favouritism towards any group or individual in the course of their work.

2.2 Employees must act with integrity at all times.

2.3 If it is suspected that a contractor, outside supplier or other person/organisation is acting in an improper manner, employees should report it to their line manager as a matter of urgency.

3. Process

3.1 Gifts

3.1.1 Employees may accept items up to the value of £10 e.g. diaries, calendars etc, usually distributed by companies as a promotional exercise.

3.1.2 Without causing offence, employees should discourage service users or other organisations from offering gifts. However, where small gifts, e.g. chocolates, are given as thanks for service provided, for example from a person in residential care can be accepted if they are shared within the team or raffled for charity.

3.1.3 If gifts have a higher value than £10, employees should tactfully refuse them. If gifts of this value are delivered, they should be returned with an appropriate explanation. If gifts cannot be returned, the senior manager should dispose of them to charity and record this fact.

3.1.4 All gifts above a value of £10 should be registered on the appropriate form, even if the gift is returned. Please see 4.1 of this procedure.

3.1.5 Gifts of cash should not be accepted.

3.2 Hospitality

3.2.1 Employees may accept incidental hospitality, such as light refreshments, tea or coffee, as offered at a visit, conference, meeting or promotional exercise.

3.2.2 Where other than incidental hospitality is offered by an existing contractor or by an organisation likely to be involved in a contract, the hospitality should be refused. Employees should avoid socialising with organisations and pay their own bills for meals, travel etc.

3.2.3 Invitations to social events offered as part of normal working life, e.g. opening celebrations, annual dinners, may be accepted if authorised by the appropriate Head of Service.

3.2.4 Invitations to any types of hospitality that are of no benefit to the authority, e.g. sporting events, must not be accepted.

3.2.5 All offers of hospitality, other than incidental, must be registered on the appropriate form, please see 4.1 of this procedure.

3.3 Inducements

3.3.1 Employees must not accept inducements, e.g. a bribe.

3.3.2 All offers of inducement must immediately be reported to the appropriate senior manager and be registered as per section 4.1 of this procedure.

4. Procedure

4.1 All offers of accepted/declined gifts or hospitality (other than incidental) must be entered on Form A (attached), together with an estimate of value, and passed to the Section Head.

4.2 Section Heads will keep Form A as a register of offers. These will be submitted to the Head of Service at the end of September and March.

4.3 The Head of Service will retain a file of higher value gifts or hospitality offered, declined or accepted. A report to DMT will be presented in April summarising the information.

4.4 Where gifts, hospitality or inducements are offered to the Head of Service, the appropriate Executive Director will sign the form.

4.5 Where gifts, hospitality or inducements are offered to the Executive Director, the form will be signed by the Chief Executive.

4.6 A central file of all gifts, hospitality or inducements offered, declined or accepted by Executive Directors or the Chief Executive will be maintained by the Chief Executive.

4.7 If any employees are uncertain how to deal with an offer of a gift or hospitality, he/she should contact their manager.

4.8 If an employee’s interpretation of this Code and/or their actions are called into question, it is the responsibility of the appropriate manager to investigate whether the person acted in good faith according to their understanding of the Code of Practice.

i) GIFTS AND HOSPITALITY FORM A

Section 4.02 GIFTS AND HOSPITALITY REGISTER 2000/2001

NAME	SERVICE AREA	OFFERING ORGANISATION	DETAILS OF GIFT/HOSPITALITY	ESTIMATED VALUE (if known)	ACCE REJE

Signed ………………………………………………….. Employee

Signed ………………………………………………….. Head of Service/Manager

APPENDIX D
June 2011

SHEFFIELD CITY COUNCIL

WHISTLEBLOWING

SEE IT – SAY IT

SECTION 1 – INTRODUCTION AND POLICY

1.1 INTRODUCTION

All of us at one time or another have concerns about what is happening at work. Usually these concerns are easily resolved. However, when they are about unlawful conduct, financial malpractice or dangers to staff, the public or the environment, it can be difficult to know what to do.

You may be worried about raising such issues or may want to keep the concerns to yourself, perhaps feeling it’s none of your business or that it’s only a suspicion. You may feel that raising the matter would be disloyal to colleagues, managers or to the Council. You may decide to say something but find that you have spoken to the wrong person or raised the issue in the wrong way and are not sure what to do next.

Sheffield City Council has introduced this policy to enable you to raise your concerns about such issues at an early stage and in the right way. We believe that enabling our employees to raise concerns safely is an important part of corporate health and we want to promote this. We would prefer you to raise the matter when it is just a concern rather than wait for proof provided you believe the concern is true and we encourage you to do so through this procedure.

The Council’s Code of Conduct for employees requires that you report genuine concerns of fraud, theft or unethical behaviour etc. This policy provides you with ways of doing that.

If something is troubling you which you think we should know about or look into, please use this policy. If, however, you are aggrieved about your personal position, please use the Grievance Procedure - which you can view on the Council’s Intranet site or get from your manager or the Human Resources Team. This Whistleblowing Policy is primarily for concerns where the interests of others or of the organisation itself are at risk.

This policy applies to employees of Sheffield City Council including those on permanent, temporary or fixed terms contracts and casual workers. School based employees are not within the scope of this policy but have a separate policy agreed by the Governing Body.

It does not apply to members of the public who should raise their concerns through the Council’s complaints procedure either online at: Customer Feedback - Online Form by telephone on 2735000 or by email at: complaint@sheffield.gov.uk

1.2 THE COUNCIL'S ASSURANCES TO YOU

Your safety

The Council is fully committed to this policy. It will be followed by managers at all levels. If you raise a genuine concern under this policy, you will not be at risk of losing your job or suffering any form of retribution as a result. Provided you are acting in good faith, it does not matter if you are mistaken. Of course we do not extend this assurance to someone who maliciously raises a matter they know is untrue.

Confidentiality

The processes of investigating any complaints or issues raised must comply with natural justice and that will often lead to disclosure of the source of the information. We will not tolerate the harassment, bullying or victimisation of anyone raising a genuine concern, however, we recognise that you may nonetheless want to raise a concern in confidence under this policy. If you ask us to protect your identity by keeping it confidential, we will not disclose it without your consent. If the situation arises where we are not able to resolve the concern without revealing your identity (for instance because your evidence is needed in court) we will discuss with you whether and how we can proceed.

Article V. Remember that if you do not tell us who you are, it will be much more difficult for us to look into the matter, protect your position or give you feedback. While we will consider anonymous reports, this policy is not well suited to concerns raised anonymously.
Article VI.
Article VII. Your right to support in meetings
Article VIII. You have the right to be accompanied by your Trade Union Representative or a work colleague who is not involved and would not be called as a witness, in any meetings, which have a connection to your whistleblowing concern. This could be
Article IX.

- Meeting a manager or Whistleblowing Contact or Co-ordinator to raise the concern
- Meeting an investigation officer in connection with the concern
- Taking part as a witness in any action taken as a result of raising the concern.

1.3 HOW TO RAISE A CONCERN IN THE COUNCIL

We hope you will feel able to raise your concern with your manager or another manager in your service area, but we know that this will not always be the case and may not be appropriate. For this reason we have provided a number of different ways to raise your whistleblowing concern and these are described in Section 2.

This section will tell you about

- How to raise a concern

- Who will receive and handle the information on behalf of the Council

- Your right to be represented or supported in any meetings

1.4 HOW WE WILL HANDLE THE MATTER

Once you have told us of your concern, we will look into it to assess initially what action should be taken. This may involve an internal inquiry or a more formal investigation e.g. by the Police or by an external regulatory body.

We will tell you who is handling the matter, how you can contact them and whether further assistance may be needed from you.

If your concern falls more properly within the Grievance Procedure we will tell you.

When you raise the concern you may be asked how you think the matter might best be resolved. If you do have any personal interest in the matter, you must tell us at the outset.

In Sections 2 and 3 we have set out what you can expect from us when we handle and respond to your concern.

1.5 INDEPENDENT ADVICE

If you are unsure whether to use this policy or you want independent advice at any stage, you may contact:

- Your union – contact details are provided in Appendix C or are available on the Council's Intranet service

- The independent charity Public Concern at Work on 020 7404 6609. Their lawyers can give you free confidential advice at any stage about how to raise a concern about serious malpractice at work.

1.6 EXTERNAL CONTACTS

We hope this policy gives you the reassurance you need to raise such matters internally, but if you feel unable to raise the concern internally we would prefer you to raise the matter with the appropriate agency than not at all. Provided you are acting in good faith and you have evidence to back up your concern, you can also contact

- Your local Council member (if you live in the area of the Council)
- External Audit (Audit Commission)
- Relevant professional bodies or regulatory organisations
- Your Solicitor
- The Police
- Other bodies prescribed under the Public Interest Disclosure Act, eg
  - Information Commissioner's Office
  - Serious Fraud Office
  - Environment Agency
  - Health and Safety Executive

If you do take the matter outside the Council, you need to ensure that you do not disclose confidential information, or that disclosure would be privileged. You should, therefore, first check with Legal Services, who will give you confidential advice; you do not have to give your name if you do not wish to. You will find a contact telephone number in Appendix C.

1.7 IF YOU ARE DISSATISFIED

If you are unhappy with our response, remember you can use the other routes detailed in this Policy at paragraph 1.6.

While we cannot guarantee that we will respond to all matters in the way that you might wish, we will try to handle the matter fairly and properly. By using this policy, you will help us to achieve this.

SECTION 2 – RAISING A WHISTLEBLOWING CONCERN

Article X.

2.1 WHAT TYPES OF CONCERNS CAN BE RAISED

You can use the Whistleblowing Policy to raise concerns about something, involving employees or Members of the Council, which is happening at work that you believe to be

- Unlawful conduct
- Financial malpractice
- Causing a danger to staff, the public or the environment
- Contradicting the Council's Code of Conduct
- Deliberate concealment of any of the above.

We have provided some examples of the kind of issues the Council would consider as malpractice or wrong-doing that could be raised under this Policy at **Appendix B**, however, this should not be considered to be a full list.

If you are in doubt – raise it!

2.2 WHO WILL RECEIVE AND HANDLE THE INFORMATION

The council has trained and prepared members of staff to handle whistleblowing concerns. Some staff will act as **Whistleblowing Contact Officers** and will be a first point of contact for you, as an alternative to speaking to your manager. We have also named **Whistleblowing Co-ordinators,** who will be responsible for   considering or investigating the matter and letting you know what is happening.

We have tried to make roles and responsibilities as clear as possible so that you can be confident that your concerns will be addressed properly. These are set out in **Appendix A** to this policy.

The Monitoring Officer has overall responsibility for the maintenance and operation of this policy. The Monitoring Officer will report outcomes, as necessary to the Council, in a form that will maintain your confidentiality as far as possible. The Monitoring Officer is the Deputy Chief Executive. Contact details are provided at the end of this document.

2.3 HOW TO RAISE A CONCERN

There are a number of different ways to raise a whistleblowing concern. You can choose the one that suits you. It doesn't matter which, you can be assured that a named manager will properly consider it. However you decide to raise the concern, please ensure that you state that you are doing so under the Whistleblowing Policy.

If at any stage we feel that your concern is a grievance, rather than a whistleblowing matter, we will tell you.

You can:

a) Raise it with your supervisor, manager or a more senior manager in your service.

If you have a concern, which you believe is covered by the Whistleblowing Policy, we hope you will feel able to raise it first with your supervisor or manager.

If you feel unable to raise the matter with your line manager, for whatever reason, you could raise it with a more senior manager in your service.

You can do this verbally or in writing, by letter or email.

Make sure you ask for your concern to be considered under the Whistleblowing Policy.

Please say if you want to raise the matter in confidence so that arrangements can be made to speak to you in private.

(i) b) Raise it with a Whistleblowing Contact Officer

You can use any of the contact numbers listed to raise your concern in confidence. You will speak to a member of Council staff who is trained and prepared to take your call and who will pass it onto the most appropriate Whistleblowing Co-ordinator for consideration or investigation.

(b) c) Raise it directly with a Whistleblowing Co-ordinator or Council Monitoring Officer.

If you feel the matter is so serious that you cannot discuss it with your manager or a Whistleblowing Contact Officer, you can raise your concern directly with a Whistleblowing Co-ordinator or the Councils Monitoring Officer.

Concerns can be raised verbally, by arranging a meeting with the appropriate officer, or in writing by letter or email.

(c) d) Using email

There is no reason why you cannot use email to raise a whistleblowing concern. However, if you choose to use email, please take extra care to make sure that your message is sent to the correct person and consider that, due to the nature of email it may be read by other people.

Putting your concerns into an email is the same as writing a letter. To help make sure your concerns are seen and handled quickly, mark the subject box:

Whistleblowing – confidential – recipient only.

(d) e) Raising concerns anonymously

If you choose not to tell us who you are, it will be much more difficult for us to look into the matter or to protect your position or to give you feedback. While we will consider anonymous reports, our policy and procedure are not well suited to concerns raised in this way. Please take time to read the policy which sets out our assurances to you if you raise a concern under this procedure.

Article XI.

Article XII. Your right to support in meetings

Article XIII. If you are asked to attend a meeting in connection with the concern you have raised you may be accompanied in the meeting by your Trade Union Representative or a work colleague (who is not involved and would not be called as a witness), in any meetings, which have a connection to your whistleblowing concern.

Article XIV.

SECTION 3 – THE PROCEDURE

STAGE 1 - VERIFICATION

Concerns raised under this procedure may be resolved by the person that you raise them with. This could be your supervisor, manager or a more senior manager in your service. If they are not able to resolve the matter or you have raised your concern with a Whistleblowing Contact it will be referred, on the day that it is received, to the Whistleblowing Co-ordinator most appropriate to the nature of the complaint.

The Whistleblowing Co-ordinator will make initial enquiries to assess whether an investigation is required and, if so, what form it should take. Although you are not expected to prove the truth of any allegation, you will need to demonstrate that there is a sufficient reason for making initial enquiries. This policy provides protection to employees who raise issues in the genuine belief that there is serious cause for concern. If the complaint is found to be in bad faith disciplinary action may be considered.

If it is confirmed that the Whistleblowing Procedure is the appropriate route and an investigation is required, the concern will be recorded, an Investigating Officer will be identified and an investigation commissioned by the Whistleblowing Co-ordinator. The Whistleblowing Co-ordinator will tell you who will investigate and the likely timescale for the investigation.

If there is insufficient information to make a decision about the most appropriate investigation route the Whistleblowing Co-ordinator will ask you for more information.

If the Whistleblowing Co-ordinator considers that the concern falls within the scope of another procedure, such as the Grievance Procedure, they will refer it to the relevant manager for appropriate action. You will be informed which procedure will be used to address the concerns you have raised.

If it is decided not to investigate further you will be told what enquiries have been made and the reasons for the decision.

When any meeting is arranged to discuss your concerns, you have the right to be accompanied by a Trade Union Representative or other person employed by the Council who is not involved in the area of work to which the concern relates and who also could not be called as a witness.

STAGE 2 – THE INVESTIGATION

The Investigating Officer may ask you to put your concerns in writing and provide as much evidence as possible. It may also be necessary to ask you to provide a witness statement. You will have the opportunity to confirm that it is accurate and complete.

You will be asked to agree that the information you have provided and your name may be disclosed so that we can decide how the Council will respond and investigate the issue.

If you do not want to disclose your identity the Whistleblowing Co-ordinator will decide how to proceed in consultation with the Monitoring Officer.

The Investigating Officer may need to contact you or other witnesses during the investigation.

The investigation will be carried out as quickly as possible but the time taken will depend on the nature of the matters raised and the availability and clarity of the information required. You will be updated at 28 day intervals unless this is not practicable.

If you are required to take part in the investigation you have the right to be accompanied by a Trade Union Representative or other person employed by the Council who is not involved in the area of work to which the concern relates and who also could not be called as a witness.

STAGE 3 – THE OUTCOME

The investigation will be concluded with a written report of enquiries made, the findings on the strength of the evidence and whether the substance of the allegations has been established. If the investigation concludes that the allegations are not substantiated the report will conclude whether the concerns were raised in good faith.

The report will include appropriate recommendations and will be presented, in the first instance, to the commissioning Whistleblowing Co-ordinator. They will be responsible for ensuring it is presented to the appropriate officers, internal and external bodies.

Where legal and confidentiality constraints allow, you will receive information about the outcome of any investigation.

The Council will take steps to minimise any difficulties which you may experience as a result of raising a concern. For instance, if you are required to give evidence in criminal or disciplinary proceedings, the Council will advise you about the procedure and will provide support.

Monitoring

A central record of all whistleblowing complaints, including dates, substantive issues, findings and outcomes is retained by Human Resources. This is provided on a regular basis to the Monitoring Officer who provides reports as necessary to the Council. The Monitoring Officer will be updated on a regular basis where cases are investigated.

ROLES AND RESPONSIBILITIES

Article XV. Monitoring Officer

The Monitoring Officer has a statutory duty to consider issues, which have or may result in the Council being in contravention of the law or a Code of Practice. For this reason the Monitoring Officer has overall responsibility for the maintenance and operation of this policy.

The Monitoring Officer will receive an updated log of whistleblowing complaints on a monthly basis including details of complaints received, action taken and analysis of trends. The Monitoring Officer will provide information relating to whistleblowing issues and trends to the Council as appropriate.

Article XVI. Whistleblowing Contacts

The Whistleblowing Contacts are trained volunteers drawn from across the Council and from each Portfolio. Their contact details are published in the Whistleblowing Policy and on the Intranet.

The Whistleblowing Contacts are responsible for

- Receiving the initial contact from the individual raising their concern
- Providing support and guidance on the policy and procedure
- Referring the complaint to the appropriate Whistleblowing Co-ordinator
- Completing reporting requirements

The Whistleblowing Contacts are trained to handle situations and individuals sensitively, fairly and promptly and to maintain confidentiality wherever possible.

Article XVII. Whistleblowing Co-ordinators

Article XVIII. The Whistleblowing Co-ordinators are named officers from the following services

- Human Resources e.g. for employment matters
- Legal e.g. for issues relating to unlawful practice
- Governance e.g. for concerns relating to decision making
- Audit e.g. for concerns relating to financial irregularity, fraud, corruption, theft
- Finance e.g. for matters relating to financial irregularity, financial mismanagement
- Health and Safety e.g. for issue about unsafe or dangerous practices
- Safeguarding e.g. for matters involving service to children and vulnerable adults
- Commercial Services.

Their role is to

- Receive complaints relating to their specific professional area referred by the Whistleblowing Contacts or directly from individual employees
- Make initial enquires and assess whether an investigation is required and, if so, what

form it should take
- If appropriate, commission the investigation, receive and consider findings
- Where the concerns or allegations fall within the scope of specific procedures (e.g. disciplinary procedure) refer them to the relevant manager for consideration under those procedures except where this may result in investigation by a person who may potentially be implicated
- Communicate with the individual who initially raised the concern to inform them of the process to be followed, progress and the outcome
- Complete reporting requirements

Article XIX. Human Resources

The Human Resources Team are responsible for:

- Development and maintenance of the policy
- Communicating and publicising the policy
- Maintaining the list of Whistleblowing Contacts and Co-ordinators and ensuring that appropriate briefing and training is provided
- Supporting investigations

Article XX. Human Resources Business Support Team

The Human Resources Business Support Team will:

- Maintain a central log of whistleblowing complaints, actions and outcomes
- Provide the updated log to the Monitoring Officer on a monthly basis including details of complaints received, action taken and analysis of trends

Article XXI.

Article XXII. Corporate Risk Management Group

The Corporate Risk Management Group will receive quarterly reports on whistleblowing issues including analysis of trends.

Audit Committee

The Audit Committee will receive quarterly reports on whistleblowing issues including analysis of trends that emerge through this and other arrangements including the grievance procedure.

The Audit Committee will also consider the operation of the policy in its annual review of governance arrangements in terms of accessibility and robustness.

Standards Committee

The Standards Committee role is to check within ethical governance frameworks (which are reviewed annually) that the policy exists and is implemented.

EXAMPLES OF CONCERNS WHICH MAY BE RAISED

This list shows the kind of issues that may be raised under the Whistleblowing Policy. However, there may be other concerns that can be raised under the policy that are not shown here. A Whistleblowing Contact will be able to advise you if you are not certain whether this is the appropriate process.

- Poor or unprofessional practice by a member of staff or an agency which results in the service user not getting the same quality of service which is available to others

- Improper/unacceptable behaviour towards a service user which could take the form of emotional, sexual or verbal abuse, rough handling, oppressive or discriminatory behaviour or exploitative acts for material or sexual gain

- Any unlawful activities, whether criminal or a breach of civil law

- Fraud, theft or corruption

- Concerns regarding possible breaches of Health and Safety Regulations

- Harassment, discrimination, victimisation or bullying of employees and/or service users

- Leaking confidential information in respect of Council activities or records

- Doing undisclosed private work which may conflict with working for the Council, or which are being carried out during working time

- Inappropriate contact with members of the public within Council facilities, or whilst carrying out Council duties or outside of working time

- Taking gifts or inducements

- Inappropriate use of external funding

- Maladministration as defined by the Local Government Ombudsman

- Breach of any statutory Code of Practice

- Breach of, or failure, to implement, or comply with any Council policy

- Misuse of Council assets, including computer hardware and software, buildings, stores, vehicles

WHISTLEBLOWING CONTACT OFFICERS

If you are unable to report a genuine concern by any of the means explained in the policy, you may choose to telephone one of your Directors' numbers as listed below. Outside normal office hours, a voicemail or answer machine facility will be in operation. Please remember that you must leave your name and telephone number at which you can be contacted.

Deputy Chief Executive Team

Alistair Griggs	Director of Modern Governance	34019
Joe Fowler	Director of Communications and Performance	34019
James Henderson	Director of Policy and Research	53126
Edward Highfield	Director of Economy, Enterprise & Skills	53126
Chris Shaw	Director of Health Improvement	53126
Lynne Bird	Director of Legal Services	34018

Resources Leadership Team

Eugene Walker	Director of Finance	35872
Julie Toner	Director of Human Resources	34081
Cheryl Blackett	Head of Human Resources, Policy & Governance	34080
Sue Palfreyman	Head of Human Resources, Service Delivery	35530
Sue Kelsey	Interim Head of Schools HR Service	2930880
Nalin Seneviratne	Director of Property & Facilities Management	34120
Paul Green	Director of Information Services	36818
Barry Mellor	Commercial Director	2053819
Julie Bullen	Director of Customer Services	36967
Kevin Foster	Director of Transformation Programme	2053478
Neil Dawson	Head of Transport Services	2037595

Children, Young People and Families

Jayne Ludlam	Deputy Executive Director of Children & Families	2930063
John Doyle	Director of Business Strategy	35663
Maggie Williams	Children’s Commissioner	2930968
Tony Tweedy	Director of Lifelong Learning, Skills & Communities	2296140

Place

John Charlton	Deputy Executive Director/Director of Streetforce	36552
Paul Billington	Director of Culture and Environment	35071
Les Sturch	Director of Development Services	35909
Mick Crofts	Director of Business Strategy	36148
Sue Millington	Senior Strategy Manager	35128
Andy Nolan	Director of Sustainable Development	36135

Communities

Eddie Sherwood	Director of Care and Support Communities	34840
Miranda Plowden	Director of Commissioning	35057
Jan Fittzgerald	Interim Director of Community Services	34486
Bev Coukham	Director of Business Strategy	35094

WHISTLEBLOWING CO-ORDINATORS

Human Resources

Cheryl Blackett	Head of Human Resources, Policy and Governance	34080
Sue Palfreyman	Head of Human Resources, Service Delivery	35530
Sue Kelsey	Interim Head of Schools HR Service	2930880

Legal

Lynne Bird	Director of Legal Services	34019

Governance

Alistair Griggs	Director of Modern Governance	36629

Audit

Steve Gill	Chief Internal Auditor	34363

Finance

Eugene Walker	Director of Finance	35872

Health and Safety

Steve Clark	OD Manager, Safety and Employee Well-being	34796

Safeguarding

Cath Erine	Service Manager	36870
Karen Bennett	Service Manager	2053846
Des Charles	Service Manager	35819

TRADE UNION REPRESENTATIVES

Jon Mordecai	UNISON	2736307
Mark Keeling	UNITE	2736486
Shelagh Carter	GMB	2768017

(Contact Officers/Co-ordinators/Trade Union Representatives last updated June 2011)

APPENDIX E

Sheffield
City Council

Policy Document

Information Security Policy

22nd September 2010

Document Control

Organisation	Sheffield City Council
Title	Information Security Policy
Author	David Bownes
Filename	Information Security Policy.doc
Owner	David Bownes – Lead Information Management Officer (Information Governance and Security Team, BIS)
Subject	Information Security
Protective Marking	Unclassified
Review date	1st January 2011

Revision History

Version	Revision Date	Reviser	Previous Version	Description of Revision
V 0.18 Draft	25/01/10	David Bownes	V0.17	Re-write to reduce volume, highlight key messages and address feedback to date
V 2.00	18/03/10	David Bownes	V0.18	Revised to include portfolio feedback
V 2.01	22/07/10	David Bownes	V2.00	Corrected Protective Marking from “RESTRICTED” to “PROTECT” paragraph 5.2 on page 5 and paragraphs 1 and 3 on page 18; re –dated the policy
V2.02	22/09/10	David Bownes	V2.01	Removed the words “and it will be logged into and out of City Council premises;” from Paragraph 10 of the Removable Device and Media Policy (Page 25); re – dated the policy
V2.03	09/12/11	David Bownes	V2.02	Added new clause 5.4 in “Applicability”

Document Approvals

This document requires the following approvals (Information Governance Board assumed membership)

Name	Role	Date Approved
Paul Green	Senior Information Risk Owner	25/03/10
Errol Simon	Head of Enterprise Architecture	25/03/10
David Bownes	Data Protection/ FOI Advisor	19/03/10
Ralph Mcnally	Solutions Architect (Information)	19/03/10
Mick Crofts	Director of Business Strategy (Place)	25/03/10
Bev Coukham	Head of Communities Development Unit	25/03/10
Peter Mucklow	Children’s Commissioner	25/03/10
James Henderson	Director of Policy and Research (DCX)	25/03/10
Kevin Foster	MEC Programme Director (Resources)	25/03/10
Anna Earnshaw	Director of IT (Capita)	25/03/10

Document Distribution

This document will be distributed to the following for review and feedback prior to submission for approval:

Name	Role	Date Issued for Review
BIS SMT	Subject Matter Experts	02/02/10
John Hendley	Place Representative	03/02/10
Andrew Crompton	CYP Representative	03/02/10
Howard Middleton	Communities Representative	03/02/10
David Hewitt	Deputy Chief Executives Representative	03/02/10
David Hill	Sheffield Homes Representative	03/02/10
Theresa Brunyee	Resources Representative	04/02/10
Julie Toner	HR Representative	03/02/10
Ann Disbury	Internal Audit Representative	
Giles Dawson	Capita Representative	03/02/10
Adele Robinson	Equalities Representative	03/02/10
Kevin Clarkson	Workstyle Representative	03/02/10
J Pascek, J Stevenson, M Keeling, K Stallard	Union Representatives	04/02/10

NB Portfolio representatives are responsible for identification of relevant stakeholders within their portfolio and onward distribution

Contents

1 Introduction

1.1 Sheffield City Council recognises that information security applied in isolation without due acknowledgement of business need is a barrier to effective information management. Information security must be an enabler with decisions based on business need to support our functions. This is the key principle by which this policy has been developed and will be subsequently implemented and maintained.

1.2 In order to ensure the continued delivery of services to our customers, we are making ever increasing use of Information and Communication Technology (ICT) and customer information held by the City Council and other public sector organisations.

1.3 The information that we hold, process, maintain and share with other organisations is a vitally important asset that, like other important business assets, needs to be suitably protected and used within a governance framework.

1.4 In order to maintain public confidence and ensure that we comply with the general law, we must maintain compliant standards of information security. A number of policies are being developed to help guarantee these standards.

2 Authority for this Policy

2.1 This policy is made by the Director of Business Information Solutions (“the Director”) using his delegated powers as set out in Item 1 in the Information Governance Board Minutes dated 7th January, 2009.

2.2 This delegation is to establish and approve internal policies dealing with all aspects of the management of all Sheffield City Council information and its security.

3 Precedence and Review

3.1 Where there is any conflict between this policy or any directions given under it with any other City Council internal policy, instruction or guideline, this policy will take precedence, except where the Director agrees otherwise after considering the law and the interests of the City Council.

3.2 The Information Governance and Security Team is responsible for reviewing this policy at least annually and for making recommendations on changes to the Director.

3.3 Where this policy or any decision made under it conflicts with any contract between the City Council and any other party, the contract terms shall take precedence in the absence of an agreement between the parties to the contrary.

4 Decision Making Under this Policy

4.1 Generally, this policy assigns decision making responsibilities to designated individuals. Where it does not or where the designated individual fails to make a decision, and a decision is required it shall be made by an Information Management Officer or a Lead Information Management Officer employed in the Information Governance and Security Team, Business Information Solutions service within the Resources Directorate.

4.2 The Director may make or review any decision under this policy and if appropriate, substitute his own decision for it.

5 Applicability

5.1 This policy applies to everyone who is authorised by the City Council to use any paper based or electronic system containing information provided for, owned, controlled or administered by the City Council ('Users'). It also applies to everyone who is authorised to use in any way information that isn't public, provided to or created by the City Council in any circumstances.

5.2 The City Council will treat all information that is not public as "PROTECT" in accordance with the HM Government Security Policy Framework. That information will be controlled so that only those with a "need to know" will be able to access it; be marked appropriately by the originator/owner where possible; where the information is an official record, treat it in accordance with the law relating to such records.

5.3 This policy applies to all information processed by, and on behalf of, the City Council regardless of form and imposes a series of controls.

5.4 The Director may modify or disapply any clause(s) in this policy in respect of any information, information system or user covered by it. Each decision made under this clause must: be comprehensively recorded in writing; and be based on an assessment of the risks of the proposed action; and state the time period during which it has effect.

Article XXIII. 6 Purpose

6.1 This document details the City Council's Information Security Policies. An objective of these policies is to ensure that consistent and high standards of information security are applied across the City Council to:

- ensure that everyone (especially citizens and users of the City Council systems) are assured of the confidentiality, integrity and availability of the information we hold;
- minimise business impact caused by security incidents;
- meet legal and regulatory requirements;
- ensure that all users are told of their information security responsibilities;
- ensure that the City Council's systems and data are used securely;
- ensure that City Council information architecture and technical infrastructure is designed and implemented to the highest industry standards;
- ensure that the City Council complies with the Payment Card Industry Data Security Standard, where appropriate.

These policies are based on industry best practice and government mandated standards. They are intended to satisfy the requirements set out by the Government Connect Secure Extranet Code of Connection (GCSx), ISO/EC 27000 Series of Information Security Standards and regulators, for example The Information Commissioner.

Article XXIV.7 Law

7.1 The following legislation governs aspects of the City Council's information security arrangements. This list is not exhaustive:

Computer Misuse Act 1990
Copyright Designs and Patents Act 1988
Data Protection Act 1998
Electronic Communications Act 2000
Environmental Information Regulations 2004
Freedom of Information Act 2000
Human Rights Act 1998
Regulation of Investigatory Powers Act 2000
Re-use of Public Sector Information Regulations 2005

8 Risks

8.1 The City Council recognises that there are risks associated with users accessing and handling information in order to conduct City Council business

8.2 This policy aims to provide mitigations for the following risks:

- citizens concerns over how the City Council uses personal data;
- failure to report information security incidents;
- inadequate destruction of data;
- inadequate control of user access to information;
- legal action against the City Council or individuals as a result of information loss or misuse;
- reputational damage following information loss or misuse;
- non-compliance with externally imposed requirements (for example, those made by Government, external audit and so on)

8.3 The City Council is currently developing a Governance framework in accordance with Cabinet Office mandated requirements. This requires the introduction of Directorate and Service Information Risk Owners and Information Asset Owners. Where policy refers to the Information Risk Owner role these responsibilities must, until Information Risk Owners are in place, be fulfilled by managers in each service.   Guidance and support may be available from the Information Governance and Security Team (01142736891).

8.4 Non-compliance with this policy could have a significant effect on the efficient operation of the City Council and may result in loss of trust, financial loss, reputational damage and an inability to provide services to our customers.

EMAIL POLICY

Sheffield City Council will ensure that its email facilities are used: lawfully and responsibly; in accordance with City Council policies and Codes of Conduct; and have appropriate security controls applied.

1 In all cases, users must act in accordance with the current Electronic Communications Policy (here) or any modification of it.

2 All email that is used to conduct or support official Sheffield City Council business must be sent using an approved email address (e.g. suffixed with .sheffield.gov.uk). Other email systems may only be used where this is critical to City Council business and formally approved by the appropriate Senior Information Risk Owner.

3 Where secure routes provided by a third party are used to send or receive email (for example, GCSx) that provider or another acting on its behalf, may monitor email traffic for lawful purposes. For example, the Government may intercept or monitor email sent through the GCSx network.

4 Before any user is given access to the GCSx network, they must have positively confirmed their acceptance that communications sent or received through it may be intercepted or monitored by Government or contractors operating on its behalf, in accordance with the law.

5 Email must only be used to disclose non-public information where this is permitted by the law, the Code of Conduct and City Council policies. Managers can provide guidance on this.

6 Users must take special care not to email malicious software to others.

7 All emails that are used to conduct or support official business must be sent using a "@sheffield.gov.uk" address or other formally approved City Council domains. All emails sent via the Government Connect Secure Extranet (GCSx) must be in the format *name*@sheffield.gcsx.gov.uk. All emails that represent aspects of City Council business or City Council administrative arrangements are the property of the City Council and not of any individual user.

8 All e-mail leaving the City Council's network through its email infrastructure will carry the following disclaimer: "This Email, and any attachments, may contain non-public information and is intended solely for the individual(s) to whom it is addressed. It may contain sensitive or protectively marked material and should be handled accordingly. If this Email has been misdirected, please notify the author immediately. If you are not the intended recipient you must not disclose, distribute, copy, print or rely on any of the information contained in it or attached, and all copies must be deleted immediately. Whilst we take reasonable steps to try to identify any software viruses, any attachments to this Email may nevertheless contain viruses which our anti-virus software has failed to identify. You should therefore carry out your own anti-virus checks before opening any documents. Sheffield City Council will not accept any liability for damage caused by computer viruses emanating from any attachment or other document supplied with this e-mail.."

9 All email will be automatically archived to the Email Archiving System after a period of three months of inactivity unless otherwise agreed by the City Council.

10 Where GCSx email is available to connect the sender and receiver of an email message containing non-public information this must be used, using automatic means where available.

11 E-mail must not be automatically forwarded to a lower classification domain. In other words, automatic email forwarding must not be used where the destination address is not capable of handling PROTECTED or a higher classification information - see the Information Asset Protection Policy for more on classification.

12 Users must implement appropriate approved access rights to their email for colleagues to support business continuity.

13 When creating an email, the information contained within it must be classified according to its content - see the Information Asset Protection Policy for more on classification.

14 Users must check destination addresses carefully before sending email; this is critically important where non-public information is being transmitted.

INTERNET ACCEPTABLE USE POLICY

Sheffield City Council will ensure that its internet facilities are used: lawfully and responsibly; in accordance with City Council policies and Codes of Conduct; and have appropriate security controls applied.

1 In all cases, users must act in accordance with the current Electronic Communications Policy (here) or any modification of it.

2 The IT Partner is responsible for the technical management of users Internet access and usage.

3 The IT Partner will ensure that all use of the internet facility is recorded.

4 The IT Partner will ensure that users will not be able to access categories of website defined by the City Council as inappropriate and will provide the facility for different groups of users to be able to see different categories of website.

SOFTWARE POLICY

Sheffield City Council will ensure the appropriate use of all software and applications by all users. This policy deals with risks associated with software deployment and use; it provides a framework to assist in the mitigation of those risks.

A key purpose of this policy is to ensure that security best practice is embedded into all application development activity – for example, any development environment and supporting processes. Managing security risks and common application vulnerabilities from the start of application development activity reduces the risks to the City Council's information and the costs of correcting insecure applications.

1 Software will never be registered in the name of an individual user. Normally, it will be registered in the name of the legal owner and/or licensee of the software.

2 A register of all software will be maintained and will include a library of software licenses. The register must contain: The title and publisher of the software; The date and source of the software acquisition; The location of each installation as well as the serial number of the hardware on which each copy of the software is installed; The existence and location of back-up copies; The software product's serial number; Details and duration of support arrangements for software upgrade.

3 Software (excluding that routinely required for everyday business purposes (such as cookies, email, etc) may not be installed unless approved by the IT Partner or Business Information Solutions using an agreed, formal change process.

4 Users must report City Council software misuse to the BIS Service Desk on 0114 273 4476.

5 All software acquired by Sheffield City Council may only be purchased through the IT Partner unless approved by the Director.

6 All software deployed by or on behalf of the City Council must be used in accordance with license conditions applying to it.

7 The IT Partner must ensure that users cannot introduce potentially harmful software such as screen savers, games, wallpaper etc onto City Council computer equipment.

8 Software must only be installed by the IT Partner once any software registration requirements have been met. Once installed, original media (where such exists) on which the software was supplied must be kept in a safe storage area maintained by the IT Partner.

9 All application development projects must apply a proven and published notation, ideally using an open standard.

10 All application development projects must produce a catalogue of development methodologies to be used.

11 All application development projects must produce a catalogue of proven and mature application development supporting tools

12 All application development projects must produce an application security architecture and apply a quality assurance process

13 All application development projects must apply integrated security testing (unit, integration and system) throughout the application development life-cycle.

14 All application development projects must control and prevent unauthorised access to the printouts or reports, electronic or hard copy, of the application source Code which makes up the programs run on systems.

15 All critical application development projects or those which are likely to pose a significant risk to production environments must be conducted in separate development/test and production environments, with access control in place to enforce separation.

16 Personnel assigned to application development projects development/test environment must not be assigned to the associated production environment as well unless the Director approves any such arrangement subject to appropriate security controls.

17 All application development projects must ensure production data (for example live payment card data or personal data) are not used for testing or development unless the Director approves any such arrangement subject to appropriate security controls. . In addition, City Council processes based on BS10012:2009 must be adhered to.

18 All application development projects must ensure the removal of test data and accounts before production systems become active.

19 All application development projects must ensure removal of custom application accounts, usernames and passwords before applications become active or are released.

20 All application Code must be written in a high-level language, using simple modular design.

21 All application Code must run with the minimum privilege settings required.

22 All application Code must individually identify individual users of the system, only permitting access to information/functions necessary for their role. If an application provides or enables the provision of public information for which authentication is specifically not required, role specific authentication will not be required.

23 All application Code must contain adequate comments to make it understandable.

24 All application Code must utilise appropriate naming standards for data items and other objects.

25 All application Code must utilise comprehensive parameter checking, especially at all entry points into sub-systems.

26 All application Code must pass all application errors to an error-handling sub-system, which will provide meaningful responses and not allow control to pass through it.

27 All application Code must provide sub-total cross-checks and appropriate audits of sensitive data, particularly when financial or personal information is processed.

28 All application Code must store sensitive information such as Payment Card Data or personal data in as few places as possible and for as short a time as possible. If such information requires long-term storage there must be documented business reasons and this data must be encrypted.

29 All application Code must protect memory areas from unauthorised access or buffer overflow.

30 All application Code must obscure all password entry fields in order to prevent passwords being viewed by others.

31 All custom Code must be reviewed (using manual or automated processes) to eliminate security vulnerabilities prior to release to production.

32 Code changes must be reviewed by appropriately qualified (ie in Code review techniques and secure coding practices) authorised personnel other than the original Code author.

33 Appropriate corrections to application Code must be implemented prior to release.

34 All Code review results must be reviewed and approved by management prior to release.

35 Public facing internet applications must be continually protected against new threats and vulnerabilities by, for example, using manual or automated application vulnerability security assessment tools or methods at least annually and after any changes.

36 Web sites must only be developed and maintained by properly qualified and authorised personnel.

37 No unauthorised changes may be made to system program source libraries.

38 Web applications (internal and external; including web administrative access to application) development projects must address the Open Web Application Security Project Guideline (http://www.owasp.org) Top 10, known as the OWASP Top 10.

39 Web browsers must not run in the context of a privileged user.

40 The IT Partner will ensure that major system upgrades are thoroughly tested in parallel with the existing system in a safe test environment that replicates the operational system where possible in line with any relevant City Council Policy.

ACCESS CONTROL POLICY

Sheffield City Council applies access controls to users of its buildings, systems and information, based on business need and associated compliance frameworks. This helps to ensure the continued confidentiality, availability and integrity of that information.

1 It is of utmost importance that passwords are protected at all times. Users must: never reveal passwords to anyone else ; never use a 'remember password' function; never write passwords down or record them anywhere else except where this is specially allowed by the City Council; never use their username within the password; comply with security rules which require, for example, frequent password changes; not use the same password for different systems either inside and outside of work.

2 It is the user's responsibility to prevent their credentials (especially passwords) being used to gain unauthorised access to City Council systems.

3 If users become aware, or suspect, that their password has become known to someone else, they must change it immediately and report their concerns to the BIS Service Desk.

4 Users must always use strong passwords for access to the computer network and password protected devices such as a Blackberry.

5 The IT Partner will ensure that strong passwords for authorised user access to the computer network are enforced; strong passwords must contain at least 8 characters and comply with at least three of the following four rules: 1 character must be upper case, 1 lower case, 1 digit and 1 symbol. In addition, as far as it is possible to do so, passwords consisting of single dictionary words must be prohibited.

6 The IT Partner will ensure that strong passwords for authorised user access to the Blackberry service are enforced; strong passwords must contain at least 7 characters and comply with at least three of the following four rules: 1 character must be upper case, 1 lower case, 1 digit and 1 symbol. In addition, as far as it is possible to do so, passwords consisting of single dictionary words must be prohibited.

7 The IT Partner will ensure that all passwords expire every 90 days (or such shorter time as the City Council specifies in the circumstances of a particular case).

8 The IT Partner will ensure that passwords provided to users (eg on initial introduction to a computer system) are changed as soon as possible - preferably before full access to the system is given

9 The IT Partner will ensure that default passwords on IT equipment or systems (for example, manufacturer provided passwords) remain in place for the minimum possible time and in any event are changed prior to installing the equipment/system onto a network.

10 The IT Partner will ensure that authorised users are not able to reuse the same password within 20 password changes.

11 The password administration process for each Sheffield City Council system must be documented.

12 The IT Partner will ensure that password and other credentials identify one user only, except where, in the circumstances of a particular case and subject to appropriate conditions, the City Council authorises different arrangements to be made.

13 The IT Partner will ensure that suitable processes exist to ensure that password and other user credentials remain secure, especially at the point of issue.

14 The IT Partner will ensure that appropriate role based system access control is implemented.

15 The IT Partner will ensure that password and other user credential administration systems are properly controlled, secure and auditable.

16 The IT Partner will ensure that where the entry of passwords is required, those passwords are displayed, where necessary, only as symbols such as dots.

17 The IT Partner will ensure that an account is automatically locked when a user makes 5 consecutive unsuccessful attempts to logon.

18 The IT Partner will ensure that a logon warning message approved by the City Council appears before the logon screen and has to be acknowledged by the user before the logon screen is presented.

19 The IT Partner will ensure that at no point prior to or during the logon process is any indication of the account privileges given.

20 The IT Partner will ensure that system administrators have individual administrator accounts that are logged and audited.

21 The Information Asset Owner of a software application is responsible for authorising all access to any information contained within it. The Information Asset Owner may exercise this responsibility by directing that designated procedures are followed.

22 The IT Partner will ensure that the level of access accorded to any authorised user accords with their role as specified in the procedures directed by the Information Asset Owner.

23 The IT Partner will ensure that the level of access cannot be changed by the user without the formal change and approval process being engaged

24 The IT Partner will ensure, as far as possible, that no unauthorised modems or other networking equipment can be connected to the City Council's network.

25 The IT Partner will ensure that remote access to the network is secured by two factor authentication methods.

26 Formal procedures must control how access to information is granted and how such access is changed.

27 Processes must be implemented to ensure that all changes to access rights of users of City Council information systems are made in a timely manner. On termination or suspension of a users employment, contract, agreement or other relationship with the

City Council, access rights must be terminated or suspended by close of business on the last working day on which access is required.

28 Access control rules and procedures must be used to regulate who can access Sheffield City Council information resources or systems and the associated access privileges.

29 Formal user access control procedures must be documented, implemented and kept up to date for each application and information system. Access control procedures must cover all stages of the lifecycle of user access, from the initial registration of new authorised users to the final de-registration of users who no longer require access.

30 Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform.

31 User access rights must be reviewed at regular intervals by Information Risk and Information Asset Owner(s) to ensure that the appropriate rights are still allocated.

32 A request for access to the City Council's computer systems must follow a procedure which requires manager, or senior officer, approval of that request.

33 Third parties must not be given access to the City Council's network without security authorisation through formal change processes. Any changes to third party connections must be made only through a formal change processes. The IT Partner must maintain a log of third party activity. The IT partner must ensure that third party connections are disabled when not in use.

34 No administrator account may be used for day to day activities where administrator level privilege is not required.

35 Where there is a business critical requirement for a specific person to have access to a defined information system without meeting all the requirements of this policy, the manager of that person may submit a request for limited access to be specially permitted. That request must be submitted in writing to the appropriate Senior Information Risk Owner. A SIRO may then decide whether or not grant the request and if so, on what terms.

36 Managers are responsible for ensuring that creation of new IT user accounts, changes in role, and termination of user accounts are notified through the standard change process in a timely manner.

37 An efficient and effective process to ensure the emergency suspension of user access must be put in place.

38 Each user of the GCSX network will be allocated a unique user identity.

HUMAN RESOURCES PRACTICE SECURITY POLICY

Sheffield City Council will ensure that users are subject to appropriate checks and information security training prior to authorising access to City Council information. This will help ensure that all recruitment is carried out in line with compliance frameworks and the continued confidentiality, availability and integrity of City Council information.

1 The information security responsibilities of users must be defined, documented and incorporated into induction processes and where appropriate, contracts of employment. "Information Security responsibilities" means responsibilities for maintaining the confidentiality, integrity and availability of the information that person will be handling and is likely to include knowledge and understanding of relevant City Council policies.

2 The City Council must satisfy itself as to the identity of potential employees and where appropriate, individuals delivering services on behalf of the City Council. It will, where this is consistent with the legal relationship or prospective legal relationship between the City Council and the individual check: at least two references; and check application forms for completeness and accuracy; and confirm claimed relevant academic and professional qualifications; and check the appearance of the individual against an official document such as a passport.

3 Where individuals have access to non-public information and/or use of the GCSX the following will also be established: proof of name, date of birth, address and signature (for example, using a passport and recent utility bill); and verification of full employment/academic history for the past 3 years; and proof of eligibility to work in the UK; and (where this is lawful) a check of unspent convictions.

4 Where access is to systems processing payment card data, credit checks on the employee must be carried out to an appropriate level as required by the Payment Card Industry Data Security Standards (PCI-DSS).

5 All contractual relationships with individuals will, as far as possible, state their own and the City Council's responsibilities for information security.

6 Each user must sign a statement confirming that they understand the nature of the information they use, that they will not use the information for unauthorised purposes and that they will return or destroy it as directed by the City Council when their formal work with the City Council terminates.

7 The City Council will ensure that all users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to comply with security policy. It will also ensure that user changes in role or business environment are carried out in a manner which ensures the continuing security of the information systems to which they have access.

8 Information Risk Owner roles will be discharged by managers if no one in the local service has been formally appointed to the Information Risk Owner role.

9 Senior Information Risk Owners must make every effort to help users to understand and be aware of information security threats and their responsibilities in applying appropriate City Council policies.

10 Managers must ensure that users: are adequately trained and equipped to carry out their role efficiently and securely; receive appropriate information security training; and updates in relevant law, policy and procedures.

INFORMATION ASSET PROTECTION POLICY

All information assets such as non-public paper records, IT equipment used to access information and the computer network must be identified, recorded and have an appointed asset owner and be appropriately protected at all times.

1 All information held by the City Council will be classified in accordance with the HMG Security Policy Framework (SPF) (http://www.cabinetoffice.gov.uk/spf.aspx) by the owner of that information asset. By default, all non-public information is in the PROTECT category; that categorisation can be changed appropriately at any time by the information asset owner. Any system subsequently allowing access to this information must clearly indicate the classification

2 Decisions on the appropriate level of access to information or information systems for a user are the responsibility of the Information Asset Owner.

3 Users who handle PROTECT information (see **1** above) will be told of the impact of loss of that information and what to do if it is lost or inappropriately disclosed.

4 The IT Partner and the City Council will ensure that non-public data which cannot be transmitted using the GCSx infrastructure and is being transferred from the City Council computer network to an external party is sent and received in encrypted form.

5 The IT Partner will ensure that proven, standard, government approved encryption algorithms, such as Triple DES and AES are used. AES should be used where possible. SSH (or better) should be used for peer-to-peer encryption.

6 The City Council and the IT Partner will ensure that where passwords are required to protect encrypted data, they are strong (as defined in the Access Control Policy) and at least 14 characters in length.

7 The IT Partner will ensure that cryptographic keys are protected against both disclosure and misuse by restricting access to as few custodians as necessary and by storing them in as few locations and forms as possible.

8 The City Council and the IT Partner will ensure that all computer equipment is appropriately located so as to minimise risk from environmental hazards, theft and unauthorised access to information contained in or accessed through it.

9 The IT Partner will ensure that business critical systems are protected by appropriate technology to reduce the risks arising from power failures.

10 The IT Partner will ensure that IT equipment is not moved or modified without authorisation.

11 The IT Partner will ensure that all IT equipment is recorded on an inventory and that inventory is kept current. The inventory must contain sufficient information about the equipment to ensure that it can easily be located, maintained and disposed of.

12 The IT Partner will ensure that all IT equipment is uniquely identifiable and that a unique asset number allocated to it.

13 The IT Partner will ensure that cables that carry data or support key information services are be protected from interception or damage. Power cables should be separated from network cables to prevent interference.

14 The IT Partner will ensure that network cables are marked and colour Coded appropriately, protected by conduit, where possible avoid routes through public areas (where possible) and installed in accordance with quality cabling practices.

15 The IT Partner must ensure that all ICT equipment is maintained in accordance with the manufacturer's instructions and with any documented internal procedures to ensure it remains in working order. Such instructions and procedures must be available to support staff when required.

16 The City Council and the IT Partner will ensure that as far as possible, hard drives in Desktop or laptop PCs do not have City Council information stored on them, except where that is necessary for the functioning of the machine. City Council information will be stored on network devices where possible.

17 Users must not be allowed to access information until the Information Risk Owner is satisfied that they understand and agree their legal and policy responsibilities for the information that they will be handling.

18 All information assets must be identified and recorded; the record must contain: type, location, owner, security classification, format, backup details, license information (where relevant).

19 All business critical information assets must have a nominated Information Asset Owner.

20 Information must be retained and disposed in line with retention and disposal schedules which comply with relevant legislation and Council policy as appropriate.

21 Information assets, the loss of which would cause significant damage to Council service delivery, will be formally owned by a Senior Information Risk owner. That person will normally be the individual who has significant operational control of the asset.

22 The City Council must document, implement and circulate formal Acceptable Use Policies (AUP) for information assets.

23 Databases holding personal information must have documented security and system management procedures which must align with the City Council's notification to the Information Commissioner of its processing of personal data (where relevant).

24 Non-public information must be appropriately protected – for example in secure network locations, identified by a risk assessment.

25 Confidential waste must be securely destroyed or made unreadable.

26 Information security arrangements must be audited regularly to provide an independent appraisal and recommend security improvements where necessary.

27 Independent security assessments, where required, must be undertaken on manual and electronic information security practices on an annual basis.

28 An on-going information security risk assessment program will be conducted on City Council business functions and services.

29 Quarterly vulnerability assessments will be undertaken on GCSx related IT equipment.

30 On-going vulnerability assessments will be undertaken on the wider IT estate.

31 All buildings used for City Council operations must be assessed for physical security.

32 Each building must have appropriate control mechanisms in place for the type of information and equipment that is stored there. Control mechanisms could include: alarms fitted and activated outside working hours; window and door locks; window bars on lower floor levels; access control mechanisms fitted to all accessible doors (where Codes are utilised they should be regularly changed and known only to those people authorised to access the area/building); CCTV cameras; staffed reception area; protection against damage - e.g. fire, flood, vandalism.

33 Access to secure areas such as the data centre and IT equipment rooms must be adequately controlled and physical access to buildings must be restricted to authorised persons. Authorised users working in secure areas must challenge anyone not wearing identification.

34 Identification and access tools/passes (e.g. badges, keys, entry Codes etc.) must identify and be used by individual authorised users only. These credentials/tools/passes must be returned when no longer required or rendered unusable or both.

35 Visitors to secure areas must sign in and out with arrival and departure times noted and be required to wear an identification badge. An employee of the City Council's IT Partner must accompany visitors accessing secure IT areas at all times.

36 Keys to all secure areas housing IT equipment and lockable IT cabinets must be stored securely away from their associated secure areas or lockable cabinets.

37 Where security breaches in secure areas occur, appropriate processes must be in place. For example, if it is necessary to terminate a users access, this must be achieved promptly and effectively - for example by disabling and recovering access cards and changing door Codes.

38 All environments must have adequate physical security applied to ensure that information assets are protected against theft, damage or unauthorised access at all times.

39 Non-public information must not be disclosed to any other person or organisation using any insecure method.

40 The disclosure of non-public information must comply with the law, regulatory requirements and City Council policy. Where regular, business critical disclosures take place, documented disclosure processes must exist.

41 Where there are reasonable grounds to suspect that non-public information is being handled inappropriately, the manager of the service responsible for that information must be notified, along with the appropriate Senior Information Risk Owner.

42 Computers will automatically lock after 5 minutes of inactivity, unless the City Council determines that a longer automatic lockout time should apply after satisfying itself that the information at risk is properly protected by other means.

43 Equipment that is to be reused or disposed of must have all of its data and software erased/destroyed in line with government standards. Data removal must be achieved by using Government approved data removing software tools.

44 Subsequent removal of equipment must be via a formal, documented process.

ACCEPTABLE USE OF PHYSICAL AND ELECTRONIC INFORMATION POLICY

All users will be told of and be expected to understand, what is acceptable use of City Council computer and telephony resources and manual information systems. This policy also requires basic security precautions (such as making sure desks are clear of non-public information when not attended).

1 In all cases, users must act in accordance with the current Electronic Communications Policy (here) or any modification of it.

2 At the end of each working period, every desk will be cleared of all non-public information.

3 Non-public information must when not in use be stored in a secure locked cupboard, drawer or other secure storage.

4 Non-public information must not be left on or in printers, photocopiers or fax machines at the end of the day.

5 Users must ensure that IT equipment is protected against unauthorised access when unattended and that portable equipment is not exposed to theft.

REMOTE AND MOBILE WORKING POLICY

Sheffield City Council will provide users with the facilities and opportunities to work remotely in a secure way as appropriate. This policy deals with risk mitigations related to remote and mobile working.

1 The IT Partner will ensure that all data on portable computer devices (including removable media devices) is encrypted to the FIPS 140-2 standard.

2 The IT Partner will ensure that an SSL or IPSec VPN is used by remote authorised users to access City Council systems by public networks, such as the Internet. If connecting to GCSx resources, this must be an IPSec-VPN.

3 The IT Partner will ensure that all remote and mobile working solutions are secured and architected in accordance with Government guidance.

4 Users must be made aware of the physical security dangers and risks associated with working within any remote office or mobile working location.

5 Equipment must not be left where it is vulnerable to theft. In the home it must also be located out of sight of casual visitors. For home working it is recommended that an "office area" of the house should be identified and kept separate from the rest of the house.

6 Users must ensure that access/authentication tokens, personal identification numbers and portable computers are kept in a separate locations.

7 The use of equipment away from a usual work site must be formally approved by the user’s manager. Equipment so used is the responsibility of the user and must: be logged in and out, where applicable; and not be left unattended in an insecure area; and (where feasible) concealed whilst being transported; and not be exposed to theft or damage at any point; and where possible, be disguised (e.g. laptops should be carried in less formal bags); and be encrypted if carrying non-public information; and be password protected (where possible); and where appropriate be adequately insured.

8 Any lost or damaged IT equipment must be reported to the BIS Service Desk.

9 Users who work remotely must ensure that portable computers are connected to the City Council network as frequently as possible and at least once every week to enable security software to be updated.

10 Users may access GCSx services, facilities or GCSx non-public information using City Council provided IT equipment only.

11 Users shall ensure that appropriate security measures are taken to stop unauthorised access to non-public information. In particular, when working in public places, users must ensure that screens are not overlooked.

12 Where the City Council permits mobile devices to access GCSX connected networks it will follow the guidance produced by Government Connect.

13 Council owned and/or supplied IT equipment must not be taken out of the United Kingdom without prior, written approval.

14 Where IT equipment and/or facilities which are not owned/supplied by the City Council are legitimately used to access City Council non-public information, the user of that equipment will be responsible for the security of that information. Users will need to ensure the appropriate configuration and use of firewalls and connectivity (especially wireless networking); the secure disposal of IT equipment; ensuring that other users of the equipment have no access to any City Council non-public information.

REMOVABLE DEVICE AND MEDIA POLICY

Sheffield City Council will ensure the controlled use of removable media devices and removable media, where these are used to store City Council information.

1 In view of the risks associated with the use of removable media devices, the City Council will only permit their use temporarily and where exceptional circumstances justify their use.

2 Only removable media devices supplied by the IT Partner may be used and they will be appropriately encrypted and protected by a strong password..

3 Users must – as far as possible - ensure that removable media devices not connected to the City Council network have up-to-date and active malware checking software prior to connecting those devices.

4 Whilst in transit or storage the data held on any removable media devices must be secured according to the classification of data held on it.

5 The IT Partner will ensure that it logs the transfer of data files to and from all removable media devices and IT equipment. Users must be made aware that this logging takes place.

6 The use of removable media devices is prohibited except as provided by this policy.

7 Users may ask to be issued with a single removable media device through a process implemented for that purpose.

8 No removable media device will be issued unless an application is made by the intended user and approved by their manager and the appropriate Information Risk Owner (if the two are different).

9 A business case supporting the issue of a removable media device must be made by the intended user of the device. As a minimum, the case must assert that: the device will permit simple, effective and efficient access to information away from the City Council network; and critical business activities will be adversely affected if the requested device isn't issued.

10 A risk assessment supporting the issue of a removable media device must be made by the user. As a minimum this must assert that: the device will be encrypted so unauthorised access will be very difficult or impossible; and it will be further protected by a strong password which will be used in accordance with City Council security policies; and the user agrees to take special care of the device to minimise the risk of theft or loss.

11 Due to the risks associated with removable media devices such as data loss, corruption, destruction or malfunction, devices must not be the only place where data required for City Council purposes is held. Copies of any data stored on removable media must be returned to the live system at the first opportunity, where appropriate.

12 Removable media devices must not be used to store non-work information; or to hold City Council information that is not required for work purposes.

13 Removable media devices that are surplus or damaged must be disposed of securely, in line with government standards – this must be arranged through the Service Desk.

14 Damaged or faulty removable media devices must not be used; the BIS Service Desk should be notified of the damage immediately.

15 Prior to re-issue of a removable media device, all data on it must be erased to government (CESG) standards. – this must be arranged through the IT Partner.

16 Removable media devices must not to be used for archiving or storing records as an alternative to other storage facilities such as networked file shares.

INFORMATION SECURITY INCIDENT POLICY

Sheffield City Council will ensure that it reacts appropriately to security incidents relating to information controlled by the City Council

1 All users must immediately report any actual or suspected breaches in information security that affect business data, or any loss of data in relation to this policy to the BIS Service Desk.

2 GCSx related security incidents will, where appropriate, be reported by the City Council to GovCertUK.

3 The City Council and the IT Partner will agree and implement an Information Security Incident Management Procedure.

4 The City Council and the IT Partner will maintain a proactive and reactive stance in relation to security incidents; both will actively prevent security incidents from arising and have adequate processes in place to deal with any that do.

5 The City Council will maintain membership of a suitable Warning Advice and Reporting Point (WARP) where such is available and use other support networks where appropriate.

IT COMMUNICATIONS AND OPERATIONS POLICY

Sheffield City Council will ensure the protection of its ICT service against malware, unauthorised changes, data loss and information leakage.

1 Connections to the City Council network infrastructure must only be made in a controlled manner. Network management is critical to the provision of City Council services.

2 The IT Partner will ensure that out-of-band administrative console access should be provided wherever possible. Where this is not feasible, encryption (SSH) must be used.

3 The IT Partner will ensure that workstations in high risk areas such as desktop computers located in public facing reception areas are risk assessed and encryption applied if appropriate.

4 The IT Partner will ensure that all wireless networks are encrypted. The WPA2 security standard (or more secure technology) must be applied, but where this is not possible WPA may be used.

5 The IT Partner will ensure that wireless networks are tested for security on an annual basis as part of the annual IT Health Check.

6 The IT Partner will ensure that no Service Set Identifier (SSID) uses the system default name.

7 The IT Partner will ensure that the Service Set Identifier (SSID) does not include the City Council’s name or location details in it.

8 The IT Partner will ensure that the SSID is: unique; and made up of random letters (upper and lower case), numbers and special characters; and uses at least 12 characters; and is changed at least annually.

9 The IT Partner will ensure that Wireless Access Points/Adapters must: have up-to-date firmware and software; and have logging enabled; and be located in a DMZ; and be located where signal strengths meet business requirements.

10 The IT Partner will ensure that GCSX audit logs which record exceptions and other security related events are kept for a minimum of six months.

11 GCSx audit logs must contain: system identity; and user identification; and records of successful/unsuccessful login; and records of successful/unsuccessful logoff; and unauthorised application access or attempts to gain access; and changes to system configurations; and use of privileged accounts (e.g. account management, policy changes, device configuration).

12 The IT Partner will ensure that access to the logs are protected from damage (for example, intentional/unintentional alteration or deletion).

13 The IT Partner will ensure that the use made of systems (including GCSX) by authorised users is logged and monitored. The City Council and the IT Partner will agree appropriate logging and monitoring arrangements for each system.

14 Sheffield City Council workstation logging (log on\log offs) must be enabled and log files stored centrally.

15 The IT Partner will ensure that development and test environments are separate from the live operational environment.

16 The IT Partner will ensure that the environments are segregated by the most appropriate controls including, but not limited to: running on separate computers, domains, instances and networks; and different usernames and passwords; and duties of those able to access and test operational systems.

17 The IT Partner will ensure that all IT infrastructure components or facilities are covered by capacity planning and replacement strategies.

18 The IT Partner will ensure that failover implementations meet business requirements and are regularly tested to ensure effective resilience.

19 The IT Partner will ensure that IP masquerading is implemented to prevent internal network addresses from being translated and revealed on the Internet, using RFC 1918 address space. Network address translation (NAT) technologies must be used for this process.

20 The IT Partner will ensure that the IP address block used for the internal network must be one defined within RFC 1918.

21 The IT Partner will ensure that internet facing computing devices or services are subject to and pass, external penetration tests: prior to being made operational; following changes; and in any case at least once each year.

22 The IT Partner will ensure that devices or services facing/connecting to the Internet or third party networks are protected by either a managed intrusion detection system or intrusion prevention system.

23 The IT Partner will ensure that Intrusion prevention or detection systems receive and implement regular signature updates.

24 If implemented, network-based intrusion detection services will be connected to a one-way (Data-In Nothing-Out) network port.

25 The IT Partner will ensure that Internet services communicating non-public information are protected by appropriate secure technologies such as TLS/SSL.

26 The IT Partner will ensure that all HTTP and SMTP services pass through a proxy server unless other arrangements offering similar levels of security are specially agreed with the City Council.

27 All proxy servers will authenticate users and enforce access controls for each of them.

28 The IT Partner will ensure that all router configuration files are secured and synchronised (for example running configuration files (used for normal running of the routers) and start up configuration files (used when machines are re-booted) have the same secure configurations.

29 The IT Partner will ensure that all firewalls, routers and switches display a notice stating that it is unlawful to enter or attempt to enter the network without proper authorisation and not identifying the IT Partner or the City Council. This notice must appear when unauthorised access to or through the device is attempted.

30 The IT Partner will ensure that all hosts are security "hardened" to CESG standards. Operating system network services must be reviewed and those services that are not required must be disabled.

31 The IT Partner will ensure that hosts run a file system supporting access controls that limit access to only the required operations and data - FAT32 is inadequate for this.

32 The IT Partner will ensure that Servers use static IP addresses even if DHCP is used.

33 The IT Partner will ensure that elevated privileges such as administration rights are restricted to authorised users based on a business need. Unauthorised accounts with elevated privileges must be removed.

34 The IT Partner will ensure that all new computer builds and device configurations are standard and conform to government security standards where available and controls must limit configuration changes that users can make.

35 The IT Partner will ensure that applications or Operating System components, services and protocols not required by the City Council are removed or disabled.

36 The IT Partner will ensure that regular backups of essential business information must be taken to ensure that the City Council can recover from a disaster, media failure or error. An appropriate backup cycle must be used and fully documented.

37 The IT Partner and the City Council will ensure that any third parties that store City Council information are required to ensure that the information is backed up.

38 The IT Partner will ensure that data sent or received via GCSx is stored separately from other data.

39 All firewalls will be configured according to relevant Government guidance.

40 The IT Partner will ensure that public facing web applications are protected by a firewall.

41 The IT Partner will ensure that firewalls are installed, appropriately configured and maintained on all computers/devices that may be used to connect to any third party networks or security zones within the City Council network. Users must not be able to disable or reconfigure firewalls or security software.

42 The IT Partner will ensure that network connections between the City Council network and GCSx are separated by a suitably configured and functioning firewall.

43 The IT Partner will ensure that Firewall specifications are chosen according to defined business requirements and must at least meet the E3 (EAL-4) standard.

44 The IT Partner will ensure that firewalls are not physically accessible to unauthorised persons.

45 The IT Partner will ensure that firewall environments are as simple as possible. Firewalls must: run the minimum necessary services protocols and software; have the fewest ports open (consistent with business need); have superfluous services and software removed or disabled . Standardised secure firewall builds/configurations must be applied.

46 The IT Partner will ensure that firewalls apply inbound and outbound filtering, to control traffic to and from the Sheffield City Council network.

47 The IT Partner will ensure that firewall configurations are formally documented, securely backed up and operate under strict change control. Requests for changes to firewall configurations must be made via the formal change process and only changes that do not significantly increase security risks may be implemented.

48 The IT Partner will ensure that firewall logging is enabled. The firewall logs must be reviewed at least quarterly and protected from unauthorised access/tampering.

49 The IT Partner will ensure that there is a formal process for secure backing up of firewall logs.

50 The IT Partner will ensure that any firewall system clocks are synchronized with the Sheffield City Council service infrastructure (required services for this must be locked down and not accessible from the Internet).

51 The IT Partner will ensure that administrative interfaces for firewalls are: locked down; and have access restricted to the internal management network; and use secure protocols; and use strong authentication resistant to brute-force attacks; and use strong passwords; and are not exposed to the public network.

52 The IT Partner will ensure that there is no use of generic firewall “administrator” accounts.

53 The IT Partner will ensure that firewall alerts are sent to the support team which is responsible for monitoring the firewall.

54 The IT Partner will ensure that the firewall implementation and rule-set is tested (to ensure effective rule implementation) at least every quarter.

55 The IT Partner will ensure that Insecure Internet Control Message Protocol (ICMP): traffic is restricted to prevent unauthorised mapping of the firewall and its rule-set; and broadcasts are neither routed nor responded to; and both redirects and timestamp requests are ignored.

56 The IT Partner will ensure that properly configured and maintained firewalls are in place on mobile computers and computers accessing GCSx systems and data.

57 The IT Partner will ensure that source routing is disabled.

58 The IT Partner will ensure that “any – any” firewall rules are prohibited.

59 The IT Partner will ensure that up to date anti-malware software/hardware is fully operational on all Sheffield City Council computer equipment wherever possible.

60 The IT Partner will ensure that anti -malware solutions are configured to actively check for and eliminate, malicious software activity; in particular, removable media devices and their contents must be scanned when they are connected to computer equipment.

61 The IT Partner will ensure that where conventional anti-malware solutions are not available, for example on some UNIX based systems, other counter-measures must be applied. These must be agreed in advance and must take into account the relevant CESG standards.

62 The IT Partner will ensure that all new computer Code to be used by the City Council is scanned for malware before being moved into production or being transmitted or stored on the Sheffield City Council network.

63 The IT Partner will ensure that a regularly reviewed and tested malware incident response procedure is in place.

64 The IT Partner will ensure that, as far as possible, all data entering or leaving the City Council's network is scanned for malware; this includes, for example, email and downloaded Internet content.

65 Where malware is detected on a system, the user of that system must report this to the BIS Service Desk immediately.

66 The IT Partner will ensure that service packs and patches for 3rd party applications are applied as appropriate.

67 The IT Partner will ensure that all IT equipment has critical software patches applied as soon as they become available and have passed any necessary testing. All other patches must be applied as appropriate. A patch management scheme, approved by the City Council must be put in place, adhered to and maintained.

68 Software which cannot be patched must not be used.

69 An annual health check of all City Council IT infrastructure systems and facilities must be commissioned by the IT Partner . This health check must include as a minimum: a penetration test of Internet facing services and equipment; a network summary that will identify all IP addressable devices; network analysis, including exploitable switches and gateways; vulnerability analysis, including patch levels, poor passwords and services used; exploitation analysis; a summary report with recommendations for improvement.

70 Removable computer media (e.g. tapes, disks and cassettes) used for backup purposes must be protected to prevent damage, theft or unauthorised access. Where couriers are required to transport backup media, a list of reliable and trusted couriers must be established. If appropriate, controls such as encryption or special locked containers must also be used.

71 Backup media stores must be kept in a secure environment and appropriate arrangements must be put in place to ensure future availability of data that is required beyond the lifetime of the backup media.

72 Storage media that is no longer required must be disposed of safely and securely in line with Government standards to avoid data leakage.

73 Any previous contents of any reusable storage media that are to be removed from the City Council network must be securely erased to Government standards.

74 Documented and appropriately detailed operating procedures must be used in all day to day maintenance of Sheffield City Council IT systems and infrastructure in order to ensure the highest possible service from these assets.

75 Changes to the City Council's IT systems must be controlled with a formally documented change control procedure. The change control procedure must consider and include: A description of the change and business reasons for it; and information concerning the testing phase; and impact assessments including information security, operations and risk; and formal approval process; and communication to all relevant people of the changes; and procedures for aborting and rolling back if problems occur; and process for tracking and audit.

76 All Directorates and Service areas must inform the BIS Service Desk of any new product requirements or of any upgrades, service packs, patches or fixes required to existing systems. All new products must be purchased through the IT Partner.

77 New information systems, product upgrades, patches and fixes must undergo an appropriate level of testing prior to acceptance and release into the live environment. The acceptance criteria must be clearly identified, agreed and documented and involve management authorisation.

78 Full backup documentation, including a complete record of what has been backed up along with the recovery procedure, must be stored at an off-site location in addition to the copy at the main site and be readily accessible. This must also be accompanied by an appropriate set of media tapes and stored in a secure area. The remote location must be sufficiently remote to avoid being affected by any disaster that takes place at the main site.

79 Full documentation of the recovery procedure must be created and stored. Regular restores of information from back up media must be tested to ensure the reliability of the back-up media and restore process and this must comply with the agreed change management process.

80 System documentation must be protected from unauthorised access. This includes bespoke documentation that has been created by Business Information Solutions or the IT Partner. This does not include generic manuals that have been supplied with software.

81 Effective version control must be applied to all documentation and documentation storage.

82 IT Operational staff and IT system administrators must maintain a log of their activities. The logs must include: back-up timings and details of exchange of backup media; and system event start and finish times and who was involved; and system errors (what, date, time) and corrective action taken.

83 The IT operational staff and IT administrator logs must be checked regularly to ensure that the correct procedures are being followed.

84 All computer clocks must be synchronised to ensure the accuracy of all the systems audit logs as they may be needed for incident investigation .

85 Where appropriate, controls must be put in place to protect data passing over the computer network (e.g. encryption).

86 A Mail Transport Agent (MTA), capable of sending and receiving mail using SMTP in accordance with RFC822 must be used.

87 All e-mail sent to lower protectively marked GSi domains and the Internet must be routed via the central GSi mail relay using the organisation's GSi connection.

88 If the City Council wishes to connect to other Public Sector networks that are connected to the GSi the appropriate Government Connect change control process will be used.

89 If the City Council wishes to use VOIP (voice over IP) it will consider the NIST Security Considerations for Voice Over IP Systems guidance

90 The network architecture must be documented in the form of a schematic diagram detailing the networks that will utilise the GCSx connection. This diagram MUST document all onward connections, remote access connections and stored with configuration settings of all the hardware and software components that make up the network. All components of the network must be recorded in an asset register.

DEFINITIONS

Term	**Meaning**
Government Connect Secure Extranet GCSx	An accredited and secure computer network between central government and all local authorities
Information asset	Any definable "set" of information the use of which is critical to support business activity

Term	Meaning
Information Asset Owner	The officer with significant control over and responsibility for, an information asset. An Information Asset Owner must be an employee whose seniority is appropriate for the value of the asset they own. The Information Asset Owner's responsibility and the requirement for them to maintain the asset must be formally agreed with the relevant Senior Information Risk Owner.
Information Governance and Security Team	Information Management Officers employed in the Business Information Solutions service
Information Risk Owner	The officer who owns and is responsible for mitigating the information risks for a defined work area.
Information security incident	An adverse event that has caused or has the potential to cause damage to an organisation’s assets, reputation and/or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes. Examples of information security incidents: unauthorised disclosure, theft or loss of information and/or equipment; inappropriate or excessive use of the Internet; unauthorised access to IT service or data including compromised password, password sharing or poor password management; inappropriate content detected on computer, device or network; detection or introduction of malicious Code; inappropriate or excessive use of corporate email.
IT infrastructure components	Examples include: File servers; Domain servers; E-mail servers; Application Servers; Web servers; Printers; Networks; Environmental controls including air conditioning.
IT Partner	Any person or organisation in a contractual relationship with the City Council to provide IT services of whatever description.
Malicious software or malware	Software designed to infiltrate, damage, change or control computer systems without lawful authority or the owner's consent. Common examples include: worms, viruses, Trojans, spyware.
Manager	In the case of staff, their manager; for others, the member of City Council staff responsible for their access to City Council information or systems

Term	**Meaning**
Non-public information	Is any information that may not be disclosed by the Council to a particular persons for legal reasons. For example you cannot normally see someone else’s health records.
Public information	Is any information freely available to anyone such as Council leaflets, application forms, advertisements and so on
Removable **media**	Data storage media such as: CD; DVD; other optical discs; media cards (including Smart Cards and Mobile Phone SIM Cards); removable computer backup devices; audio tapes.
Removable media **devices**	Any electronic device containing data storage capability which cannot be removed from the device. Examples include: External Hard Drives; USB Memory Sticks (also known as pen drives or flash drives); MP3 Players; Personal Digital Assistants (PDA’s)
The Director	The Director of Business Information Solutions (Chief Information Officer)
User	Anyone formally authorised by the City Council to use Information Assets

Policy Compliance

Failure to comply with these policies is a serious matter and users may be subject to criminal, civil or employment related sanctions (for example the misconduct process).

If aspects of this policy are not fully understood, users should talk to their manager. Guidance and support provided by the Information Governance and Security Team (01142736891).

Policy Governance

The following table identifies those accountable, etc for this policy.

Responsible – means: the person(s) responsible for developing and implementing the policy.
Accountable – means: the person who has ultimate accountability and authority for the policy
Consulted – means: the person(s) or groups to be consulted prior to final policy implementation or amendment
Informed – means: the person(s) or groups to be informed after policy implementation or amendment

Responsible	The Information Governance and Security Team
Accountable	The Director
Consulted	Everyone who is authorised by the City Council to use any system containing information provided for, owned, controlled or administered by the City Council
Informed	Everyone who is authorised by the City Council to use any system containing information provided for, owned, controlled or administered by the City Council

APPENDIX F

(A) OTHER EMPLOYMENT RELATED ACTIVITIES – FEES

Employees may be asked on occasions to give lectures or undertake work using their professional skills and expertise. If the work forms part of the duties of a post and the employee is carrying out an official duty, he/she must forward all fees to the employing directorate. Any expenses incurred will be reimbursed through the normal procedures.

Employees in receipt of ‘fees’ in respect of undertaking work and/or lecturing to an outside organisation/person(s) may retain the ‘fees’ providing:

A preparation and delivery of the work is undertaken outside working hours (unless covered below);

B equipment and/or materials are not being provided by the City Council;

C the employee is not acting as a representative of the City Council.

Where the work or lecture is undertaken during working hours the equivalent working hours must be re-arranged, in agreement with the line manager to accommodate the employee’s request or annual leave, flexi leave or time off in lieu must be used. The employee concerned may also be granted unpaid leave, subject to the agreement of the line manager in consultation with the HR Adviser.

APPENDIX G

Politically Restricted Posts (PoRPs)

Legal Background

The Local Government and Housing Act 1989 (LGHA) introduced the principle of Politically Restricted Posts (PoRPs) in local authorities. This Act had the effect of restricting the political activities of certain local authority employees. The LGHA was amended in 2009 by the Local Democracy, Economic Development and Construction Act 2009.

Restricted Posts

Posts may be politically restricted because

- they are specified as PoRPs in accordance with the legislation; or
- it has been determined that they fall within the sensitive duties related criteria of the legislation

Specified Posts within Sheffield City Council

These post holders are politically restricted without the right of appeal

Statutory Officers

The Head of the Paid Service (Chief Executive)
Director of Children's Services under Children's Act 2004 (Executive Director CYPF)
Director of Adult Services under LASSA 1970 (Executive Director Communities)
Chief Finance Officer under Section 151 of LGA 1972 (Executive Director of Resources)
The Monitoring Officer (Deputy Chief Executive)

Non Statutory Chief Officers

Officers reporting directly to the Head of the Paid service excluding secretarial/clerical support.

Deputy Chief Officers

An officer reporting directly or is directly accountable to one or more of the statutory or non statutory Chief Officers.

Officers Exercising Delegated Powers

Officers whose posts are specified by the authority in a list maintained in accordance with section 100G (2) of the Local Government Act 1972.

Assistants for Political Groups

Sensitive Duties Posts within Sheffield City Council

The duties of a post under a local authority fall within this subsection if they consist of or involve one or both of the following sensitive duties i.e.

- **giving advice on a regular basis to the authority itself, to any committee or sub-committee of the authority or to any joint committee on which the authority are represented; or where the authority are operating executive arrangements, to the executive of the authority, to any committee of that executive; or to any member of that executive who is also a member of the authority**

- **speaking on behalf of the authority on a regular basis to journalists or broadcasters**

These post holders can appeal against political restriction on the grounds that the criteria have been wrongly applied.

Teachers and Headteachers are exempt from political restriction, whatever their role.

A list of all Politically Restricted Posts within Sheffield City Council is held by the relevant Proper Officer (Chief Executive). Any modifications to this list must be reported and recorded accordingly.

Restrictions on Post Holders

Employees in PoRPs are debarred from standing for or holding elected office as

- Local councillors
- MPs
- MEPs
- Members of the Welsh Assembly
- Members of the Scottish Parliament

These restrictions are incorporated as a term in the employee's contract of employment under Section 3 of the Local Government (Politically Restricted Posts) Regulations 1990.

They are also restricted from

- Canvassing on behalf of a political party or a person who is or seeks to be a candidate

- Speaking to the public at large or publishing any written or artistic work that could give the impression that they are advocating support for a political party

Appeals against inclusion on the list of politically restricted posts

Post holders who are politically restricted because they hold specified posts have no right of appeal.

- Appeals are made to the Head of Paid Service

- Post holders of sensitive posts that are politically restricted may appeal on the grounds that the authority has wrongly applied the duties-related criteria

- Appeals may be made by the current post holder or by an individual who has been offered employment in a politically restricted post

- There is no timescale during which a post holder must make an appeal

- To appeal, employees should send a letter formally seeking exemption and a job description to the Monitoring Officer (Deputy Chief Executive), Town Hall, Pinstone Street, Sheffield, S1 2HH

- If the appeal is successful, the Monitoring Officer will notify HR Connect at Capita, so that it may be noted on the records for the individual and for the post

Please Note: This document is a summary, if you require further details or are unsure about any of the content please contact the Director of HR, Town Hall, Pinstone Street, Sheffield S1 2HH.

APPENDIX H

DIGNITY AND RESPECT AT WORK POLICY

1 OUR COMMITMENT

1.1 Sheffield City Council is committed to promoting a positive working environment where staff conduct themselves in a way which contributes positively to their team's work targets and which respects all colleagues and customers.

1.2 The Council is committed to promoting dignity and respect, to which employees are entitled. It seeks to provide an environment of mutual trust and respect amongst the entire workforce and to resolve any issues or difficulties at work in a mutually beneficial way.

1.3 It is opposed to and will not tolerate any form of harassment, discrimination, victimisation, bullying or intimidation or any unacceptable conduct towards an individual or group, in the workplace, whether a single incident or persistent acts.

2 HARASSMENT, DISCRIMINATION, VICTIMISATION AND BULLYING

2.1 The City Council has taken into account the information contained within relevant EU Directives, Employment regulations, Equality legislation and the Equality Act 2010 in determining the definitions of Harassment, Discrimination, Victimisation and Bullying.

2.2 The Equality Act covers the same groups that were protected by previous equality legislation and extends some protections to characteristics that were not previously covered, and also strengthens particular aspects of equality law. These are now called ***'protected characteristics'*** and cover Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion or Belief, Sex and Sexual Orientation

NB: People may also experience Harassment, Discrimination, Victimisation and Bullying which may not be related to a Protected Characteristic

2.3 **Definitions**

- **Harassment is** 'unwanted conduct related to a relevant *protected characteristic*, which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating or offensive environment for that individual'*.*

- **Discrimination is** 'where one person is treated less favourably than another person was or would have been treated on the grounds of their *protected characteristic'*

- **Victimisation is** ‘when an employee is treated badly because they have made or supported a complaint or raised a grievance under the Equality Act and/or Council policies' or because they are suspected of doing so.
- **Bullying is** 'persistent unwelcome offensive and intimidating behaviour or misuse of power which makes the recipient feel upset, threatened, humiliated or vulnerable and undermines their self-confidence'.

2.4 **Types of Discrimination and Harassment**

Direct discrimination
This is when someone is treated less favourably than another person because of a *protected characteristic* they have or are thought to have, or because they associate with someone who has a protected characteristic.

Associative Discrimination
This is direct discrimination against someone because they associate with another person who possesses a *protected characteristic*.

Perceptive Discrimination
This is direct discrimination against an individual because others think they possess a particular *protected characteristic*. It applies even if the person does not actually possess that characteristic.

Indirect Discrimination
Indirect discrimination can occur when you have a condition, rule, policy or even a practice in your organisation that applies to everyone but particularly disadvantages people who share a *protected characteristic*. Indirect discrimination can be justified if you can show that you acted reasonably in managing your business, i.e. that it is ‘a proportionate means of achieving a legitimate aim’. A *legitimate aim* might be any lawful decision you make in running your business or organisation, but if there is a discriminatory effect, the sole aim of reducing costs is likely to be unlawful. Being proportionate really means being fair and reasonable, including showing that you’ve looked at ‘less discriminatory’ alternatives to any decision you make.

2.5 Harassment, discrimination, victimisation and bullying can come in many forms. It may happen once or more than once, either way it is unacceptable. Examples could include:

Offensive material, including pornography, racist material, or material which ridicules or abuses religion or belief, men or women, black people, disabled people, transgender people, lesbians or gay men, older or younger people.

Verbal abuse, including racist or sexist language, and language that undermines or ridicules e.g. disabled people, lesbians or gay men, older or younger people.

Bullying, exercising power to intimidate, ridicule or demean an individual or group of people usually through a number of small incidents over a period of time.

Leering, comments on dress or appearance, embarrassing remarks or jokes, demands for sexual favours.

Physical assault, including touching or unwanted physical advances.

Persistent comments, which undermine or undervalue a person's abilities, particularly on the basis of his/her sex, race, disability, sexuality and/or age. This could also relate to comments on a persons physical appearance.

Cyber-bullying, is when the internet, phones, or other devices are used to send or post text or images intended to hurt or embarrass another person. It may include threats or sexual remarks or ganging up to make someone a victim of ridicule in social networking forums.

3 HATE CRIME AND HATE INCIDENTS

3.1 A Hate Incident is: “Any incident, which may or may not constitute a criminal offence, which is perceived by the victim or any other person, as being motivated by prejudice or hate.”

3.2 Hate Crime is defined specifically as: “Any Hate Incident, which constitutes a criminal offence, perceived by the victim or any other person, as being motivated by prejudice or hate.”

3.3 As an employee complaints of Hate Crime or Hate Incidents will be dealt with through one of the following procedures:
<u>Dignity and Respect Procedure</u> – this should be used if they feel they have experienced harassment, discrimination, victimisation or bullying at work by another Council employee.
<u>Grievance Procedure</u> – this should be used if an employee wants to raise significant and specific concerns about their employment or treatment at work.
<u>Accident, Violent Incident or Near Miss Report Form</u> this should be used if a Hate Crime or Hate Incident happens to an employee, one of their colleagues or a member of the public.
<u>Whistleblowing Procedure</u> - this should be used for concerns where the interests of others or of the organisation itself are at risk.

4 ROLES AND RESPONSIBILITIES

MANAGERS

4.1 Every Sheffield City Council manager and supervisor has a duty to implement and enforce this Policy in a fair and equitable way and to ensure that all employees for whom they are responsible understand and follow it.

4.2 Managers are responsible for ensuring that all employees are aware that breach of this Policy could lead to consideration of formal disciplinary action or dismissal under the City Council's Disciplinary procedure depending upon the circumstances.

4.3 Managers need to recognise that the lodging and/or investigation of a complaint is extremely difficult and distressing for both the complainant and the subject of the complaint. In both cases, appropriate support needs to be provided before, during and after an investigation.

4.4 Managers need to ensure that complaints of harassment, discrimination, victimisation and bullying are taken seriously and that investigations are, so far as is possible, managed speedily, confidentially and communicated effectively.

4.5 Managers need to ensure that employees, who have raised concerns or have provided evidence during an investigation, are not victimised as a result of their actions.

EMPLOYEES

4.6 Every Sheffield City Council employee has a responsibility to treat all colleagues and service users with dignity and respect.

4.7 Employees, including managers, need to be aware of their own conduct and behaviour and how it can impact on others within the workplace.

4.8 Employees are encouraged to bring to the attention of Managers any examples of unfair treatment they have witnessed or strongly suspect is taking place. This could also include the conduct of managers.

4.9 Employees are required to co-operate with investigations into allegations made under this policy.

4.10 Employees must not make false or malicious allegations and need to be aware that disciplinary action may be considered in such circumstances.

HUMAN RESOURCES

4.11 Human Resources staff will be available as a resource to Managers and Employees to provide support and guidance on the operation of this policy.

4.12 Human Resources Officers will be involved in advising Managers on the investigation of complaints however they will not take over the management of the process. It is the Managers responsibility to manage.

4.13 Employees who are experiencing problems can approach Human Resources in confidence for advice and support.

CONTACT ADVISERS

4.14 Contact Advisers are available as a point of contact for those experiencing or witnessing harassment, discrimination, victimisation or bullying at work.

4.15 Contact Advisers can provide confidential support and will assist employees in understanding the options for dealing with their particular situations.

4.16 Contact Advisers are also available as a point of contact for the subject of a complaint, but not both parties to the same complaint. They will support people from various Portfolios.

Article XXV. TRADE UNIONS AND OTHER SOURCES OF SUPPORT

4.17 Employees who are members of a recognised trade union have the right to be represented by their Trade Union representative.

4.18 Trade Union representatives can offer advice and support to employees who may be experiencing problems or have had allegations made against them.

4.19 Employees can also seek support from Staff workers Forums and colleagues.

5 WHAT WE WILL DO

5.1 The City Council will take any allegations made by employees seriously and, so far as possible, complaints will be managed speedily, confidentially and communicated effectively.

5.2 Every effort will be made to resolve complaints informally. Where this is not appropriate or possible, an appropriate manager will ensure a formal investigation will take place.

5.3 The City Council will communicate with employees to raise awareness about Dignity and Respect. The policy will also be promoted including the implications of certain behaviours.

5.4 We will support employees who experience difficulties through the provision of Contact Advisers and Human Resources professionals and ensure that Managers are updated regularly on their responsibilities under this policy and procedure.

5.5 We will ensure a system is in place to monitor and review the use of the Policy and Procedure. There will be statistical monitoring to identify potential problems and areas for improvement.

This page is intentionally left blank