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. Read Declaration of Interests Policy (DO!) Appendix A

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. See Declaration of Interests Policy~~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. See Declaration of Interests Policy (DOI) Appendix A.

~~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~~ the Declarations of Interest Policy (DOI), **Appendix A**. If you are not sure, you should ask your manager to help you.

Formatted: Font: Bold

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 AND SOCIAL NETWORKING

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.

5.5 You are personally responsible for content that you publish on-line and must follow the Social Networking Policy, **Appendix F.** You must take time to read the Social Networking Policy and understand your responsibilities and behaviours expected, when using social networking in a personal or work capacity. Ask you manager if you are unsure about the Social Networking Policy and Guidance.

Formatted: Font: Bold
Formatted: Font: Not Bold

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. See Declaration of Interests Policy, **Appendix A.**

Formatted: Font: Bold

~~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 a Voluntary Reserve Forces - ~~the~~ Reservists and Adult Instructor of ~~Territorial Army~~Cadets
- 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 HC**. 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 IH**

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 Before you start working for us, you must tell us about any unspent criminal convictions, cautions, warnings, reprimands, binding over or other orders, pending prosecutions or criminal investigations.

If you are applying for a role, which involves working with children and vulnerable adults and your job is covered by the Rehabilitation of Offenders (Exceptions) Order 1975 (Amendment) 2013, you must follow our guidance on 'declaration of criminal convictions and cautions' at the application stage and tell us about:-

- All filtered convictions and cautions for any roles, where you have to complete an enhanced Disclosure and Barring Service(DBS) **with no** barred lists check.Please see guidance on declaration of criminal convictions and cautions for the filtered list.

OR

- All convictions and cautions for any roles, where you have to complete an enhanced Disclosure and Barring Service (DBS) **with** barred lists check.

Formatted: Indent: First line: 0 cm
Formatted: Font: Arial, 12 pt
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.27 cm + Indent at: 1.9 cm
Formatted: Font: Arial, 12 pt, Bold
Formatted: Font: Arial, 12 pt
Formatted: Indent: First line: 0 cm
Formatted: Font: Arial, 12 pt
Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 1.27 cm + Indent at: 1.9 cm
Formatted: Font: Arial, 12 pt, Bold
Formatted: Font: Arial, 12 pt

If you are unsure about which criminal convictions and cautions that you need to tell us about, please ensure that you contact the recruiting manager for further advice.

~~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.~~

~~16.5~~ 16.2 When employed by us,~~Y~~ you must tell your manager if you have any criminal proceedings pending against you, if you are bound over, receive a conviction, caution, reprimand or warning.~~:~~

~~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 use your own vehicle for Council Business and carry passengers, you must also tell your manager about any driving offences or pending driving offences.

16.~~5~~4 If you do not tell us about your criminal record as listed in 16.1-16.4 above, this may be treated as possible gross misconduct and might lead to disciplinary action – including possibility of dismissal without notice.

16.6 If you are required to provide us with your Disclosure and Barring Service (DBS) Certificate, we will ask you to:-

- Complete a DBS Application Form
- Or give written permission for us to check your status on-line
- Or give permission for us to view your personal file of a previous/other role within the Council to check the outcome from a recent Enhanced DBS check.

You must bring in your DBS Certificate to show and discuss with us, when required.

16.7 It is against the law for us to employ you or allow you to volunteer for work with children and vulnerable adults, if you are listed as barred for this type of work

16.8 Once employed by us, you must tell your manager immediately, if you know that you are on, or will appear on, one or both of the DBS barred lists.

Formatted: Indent: Left: 0 cm, First line: 0 cm

Formatted: Indent: First line: 0 cm

Formatted: No bullets or numbering

Formatted: Indent: First line: 0 cm

Formatted: Font: Arial, 12 pt

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: Font: (Default) Arial, 12 pt

Formatted: Font: (Default) Arial, 12 pt

Formatted: Indent: Left: 0.63 cm

Formatted: Indent: Left: 0 cm, First line: 0 cm

16.9 If you have been barred from working with children and/or vulnerable adults and you seek employment to do so, this is a criminal activity and against the law and you will be dismissed without notice and immediately reported to the Police Authority.

~~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.~~

~~16.6 You must toll your manager if you have any criminal proceedings ponding against you.~~

~~Formatted: Indent: Left: 1 cm, No bullets or numbering~~

~~16.7~~ 16.10 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.

~~Formatted: No bullets or numbering, Tab stops: Not at 2.54 cm + 3.81 cm + 5.08 cm + 6.35 cm + 7.62 cm + 8.89 cm + 10.16 cm + 11.43 cm + 12.7 cm + 13.97 cm + 15.24 cm + 16.51 cm + 18 cm~~

17.0 ALCOHOL, DRUGS AND SUBSTANCES~~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 ismay ~~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 substances, 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 APPENDICES

A ~~Definition of what constitutes a membership of Secret Society~~Declaration of Intersts Policy

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 Social Networking Policy

G Other employment related to activities – fees

H~~G~~ Politically Restricted Posts

I~~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

Formatted: Right

APPENDIX A

Sheffield City Council

Policy and Procedure

Declaration of Interest

Publication Date: April 2014

Author: HR Specialist Service

Formatted: Font: 20 pt

Formatted: Font: 20 pt

Formatted: Font: (Default) Cambria

Declaration of Interest - Policy and Procedure

Policy

1. Introduction

1.1 All customers are entitled to the highest standards of fairness and equity from all employees providing our services. This Policy and Procedure exists to protect you and service users against any allegations of favour or disadvantage.

1.2 It is important that employees and the Council are protected from accusations of impropriety. Therefore an employee must declare any interest to their manager that they may have with any organisation, services, activity or person that may cause a direct or indirect conflict of interest with their employment or that may bring the Council into disrepute. In case of doubt, employees should always complete and submit a Declaration of Interest Form. For example:

- Employees should ensure they declare financial interest in order to comply with their statutory duty under Section 117 of the Local Government Act 1972
- In many cases the interests may not create a conflict or the fact that they are known interests will allow the individual's manager to ensure they are not placed in a position where conflict could arise.
- Every Head of Service, Director and Executive Director is responsible for ensuring their managers and staff are aware of the need to make declarations. Any monitoring will comply with all relevant laws.
- It is not possible to give comprehensive examples or detailed definitions of everything that might give rise to a conflict of interest between their duties and these interests or their ability to carry out their role effectively

1.3 Any potential conflicts of interest will be recorded in accordance with the Declaration of Interest Procedure.

1.4 The Council's Monitoring Officer will review any declarations (or a random selection of) that have been made every year. If the Monitoring Officer needs to make declarations, the Chief Executive will review them every year.

1.5 If an employee fails to follow the requirements of this policy or procedure they may be subject to disciplinary action.

1.6 Any employee, who considers they have been unfairly treated under the terms of the policy, may raise a grievance under the Council's Individual Grievance Procedure. The grievance should be submitted to their line manager or with the person making the decision.

2. Scope

2.1 This policy applies to all non-school based employees. The Policy adopted by the relevant Governing Body will apply to employees within schools.

3. General Declaration of Financial and Other Interests

3.1 As an employee of Sheffield City Council, you have a legal duty to declare any financial or other interest in an existing or proposed contract or any proposed or existing council activity or service which could cause potential conflict. This declaration includes involvement with voluntary organisations, which the council supports and/or services carried out for the council by its commercial partners, for example Capita, Kier, Amey and other similar partner organisations.

3.2 You have a legal duty to declare any interest 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, and activity or person.

3.3 If the Council has sponsored an event or a service, you must inform your line manager if you may benefit from it in any way. You must also tell your line manager if you are aware that anyone connected with you will benefit from it (this includes your relatives, your partner or spouse, or any business associates you may have).

3.4 You must declare an interest if anyone connected with you will benefit from the position you hold in the Council. This includes your relatives, your partner or spouse, or any business associates you may have. This is to ensure the status gained from working for the council is not utilised to influence a member of the public's choice when commissioning work or a service.

3.5 If you apply for a service or make representations for services on behalf of relatives, colleagues or friends or people with whom you have a close relationship, you must declare an interest where your employment position gives you significant influence.

3.6 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 over or responsibility for or to improve the chances of success of an agency within a tendering process .

4. Declaration of Membership of Organisations Not Open to the Public

4.1 You must declare and provide information about any organisation in which you have a personal interest that is not open to the public which requires formal membership, oaths of allegiance and has secrecy about rules, membership or conduct.

4.2 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:

Formatted: Font: 12 pt

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.

5. Declaration of Secondary Employment or Engagement in Other Business or Voluntary Work

5.1 If you have secured other employment or voluntary work whilst you are working for the Council, you must first complete a 'Declaration of Personal Interest Form – Appendix 1'. Your manager should respond within the agreed timescale and advise if there may be any possible conflict of interest before you commence the work. This includes paid work for another employer and working in a self-employed or business partnership basis.

5.2 If you do undertake other work you must ensure the additional hours do not impact on your performance of your duties undertaken for Sheffield City Council.

5.3 When considering undertaking other work, consideration must be given to compliance with the statutory requirements of the Working Time Regulations. The council must be made aware of any additional work that could mean you exceed an average of 48 hours of work in total in a week

5.4 Those undertaking additional work outside the authority must sign a Working Time Regulations 'Opt out Agreement' and to confirm they understand the health and safety implications of working excessive hours. This must be held on your personal file in HR Connect.

5.5 You must not refer to your role in Sheffield City Council in any promotional material which may be used to assure members of the public or give credence to another organisation.

5.6 The Council accepts no liability for your other work or engagement in other business or voluntary work and will not be responsible for any payments, expenses or demands however incurred.

5.7 With regard to any other work or engagement in other business or voluntary work you are responsible for:-

- ensuring that you have the correct insurance; and
- that you are registered with the relevant professional or regulatory bodies; and
- that you pay any tax, national insurance, or other statutory payments due; and
- for ensuring that you have the correct membership of trade or professional organisations; and that you comply with any statutory requirements or professional or trade codes of conduct.

5.8 There may be circumstances where SCC may need to retract permission for example

- Where attendance or timekeeping is of concern and may be attributed to you undertaking other work
- Where your performance falls below an acceptable standard and may be attributed to you undertaking other work
- Where a new conflict of interest arises that previously did not exist *or where a conflict later becomes apparent for any reason*

6. Reporting of Declarations of Interest

6.2 If you think there might be a conflict of interest, you must speak to your line manager to see if a Declaration of Interest Form needs to be submitted to their Head of

Service.

6.3 All Declarations of Interest must be recorded in accordance with the Declaration of Interests Procedure.

Procedure

1. You must complete a 'Declaration of Personal Interest Form' before you undertake other work or become aware of a potential conflict of interest.

2. The Declaration of Interest form will be submitted by your line manager to the HOS/Service Manager within 5 working days of receipt.

3. Your Head of Service/Service Manager will be responsible for forwarding an electronic version of the completed and agreed DOI forms to the Monitoring Officer to ensure adherence with the Policy and the Annual Governance Procedure. Copies of the completed forms should be retained by both the line manager and the employee completing the form.

4. All information supplied will be kept in confidence in accordance with the requirements of the Data Protection Act 1998 and **will only** be used for the purposes of determining if a conflict of interest arises and/or for taking any necessary decisions or actions under this policy.

5. For the purpose of considering whether there is any conflict of interests, the Council may need to contact any other organisation or individual whose details you have provided on your Declaration Form or in any updated information that you have provided. Your line manager would seek permission from yourself first before this action takes place.

6. A new declaration must be made in writing and submitted to your manager within 28 days if there is a change in circumstances. See Section 3 of the Policy.

7. For declarations relating to financial and other interests you must give an explanation as to the way you or someone connected with you may benefit.

8. For declarations relating to membership of an organisation not open to the public you should provide information about such an organisation including details of the purpose behind the organisation wherever possible. However, if this act would cause a breach in confidentiality or the organisation's protocols they you should discuss this with your line manager, who may need to seek further advice from Human Resources.

   Additionally, SCC would expect that such membership would not be in conflict

Formatted: Font: 12 pt
Formatted: Font: Arial, 12 pt
Formatted: Font: Arial, 12 pt
Formatted: Font: Arial, 12 pt
Formatted: Font: Arial, 12 pt
Formatted: Font: Arial, 12 pt
Formatted: Font: Arial, 12 pt
Formatted: Font: Arial, 12 pt

with your role with SCC. You should seek advice from your manager or Human Resources if necessary.

9. For declarations related to participation in other work or engagement in other business or voluntary work, you should provide details of the name of the organisation for which the work is undertaken and give a description of the activity concerned and potential number of hours to be undertaken.

10. If you are in any doubt as to whether an interest constitutes a conflict (this could be an actual or potential conflict, or something that could be perceived to be a conflict by a third party) then you should declare the interest on the form and your manager will determine what action is appropriate.

Formatted: Font: Arial, 12 pt

Formatted: Font: Arial, 12 pt

~~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)	ACCEPTED/ REJECTED	REASON

Signed …….. Employee

Signed …….. Head of Service/Manager

APPENDIX D

October 2012

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. Employees are generally precluded from being able to whistle blow about breaches of their own employment contract and should use the grievance procedure. If you are complaining that you have suffered harassment, discrimination, victimisation or bullying at work please use the Dignity and Respect Procedure which is on the intranet. If, however, your concern is about the dignity and respect of others then it may be appropriate to use this

procedure. 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

Section 4.03 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 reasonably believe that you are disclosing information in the public interest. It does not matter if you are mistaken. This is regarded as a protected disclosure. Of course we do not extend this assurance to someone who maliciously raises a matter they know is untrue. Whistleblowers are also protected from suffering a detriment, bullying or harassment from another employee.

Section 4.04 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.

Information and support
The Council has a number of Contact Advisors who can provide advice and information to help you explore the appropriate routes to raise your concern. The Contact Advisors can also provide support as the investigation progresses.

If you are a member of a recognised Trade Union your Trade Union can also support you.

Article VI. Your right to support in meetings
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.

The meetings you may be required to attend are:
Article VII.

- 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 or the Dignity and Respect 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 IF YOU ARE THE SUBJECT OF A COMPLAINT UNDER THIS POLICY

If you are the subject of a complaint under this policy and procedure you have the right to be accompanied by your Trade Union Representative or a work colleague at any meetings relating to the complaint but this should not be your line manager as they may be required to implement any recommendations that come out of the investigation.

The Council's Contact Advisors can provide support and guidance about the whistleblowing procedure and investigations to both parties. You can access that support if you have whistleblowing allegations raised against you.

If you are the subject of a complaint or investigation under this policy your confidentiality will be respected as with any other procedure.

1.6 INDEPENDENT ADVICE

If you are unsure whether to use this policy or you want independent advice at any stage, you may contact:

- A Whistleblowing Contact – contact details are provide in Appendix C or on the intranet
- 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.

1.7 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. If you reasonably believe that you are disclosing information in the public interest 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.

1.8 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.

If you are unhappy with the way you are treated when raising your concern or during the investigation, you can raise this under the Grievance Procedure or under the Dignity and Respect procedure as appropriate but you should not use these alternative procedures to raise the same issues that you raised in your original whistleblowing complaint.

SECTION 2 – RAISING A WHISTLEBLOWING CONCERN

Article VIII.

2.1 WHAT TYPES OF CONCERNS CAN BE RAISED

You can use the Whistleblowing Policy to raise concerns about something, involving employees, 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 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 Standards Committee, in a form that will maintain your confidentiality as far as possible. The Monitoring Officer may delegate this responsibility to the Deputy Monitoring Officer. 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 or a complaint about dignity and respect, rather than a whistleblowing matter, we will tell you.

You or your trade union representative on your behalf 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 (for example, they may be involved in the issue that you are concerned about), you could raise it with a more senior manager in your service or you can use one of the alternative options below.

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

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 who will allocate it to an appropriate Whistleblowing Co-ordinator.

(c) d) Raise it with the Council's Monitoring Officer.

If you feel the matter is so serious that you cannot discuss it with any of the officers set out above you can raise it with the Councils Monitoring Officer who will allocate it to an appropriate Whistleblowing Co-ordinator.

Concerns can be raised verbally, by arranging a meeting with the appropriate officer, or in writing by letter or email.

(d) e) 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.

(e) f) 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.

Your right to support in meetings

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.

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 malicious, 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 in consultation with the appropriate service manager or Director. Where managers or Directors within the service may be the subject of the allegations then the Whistleblowing Co-ordinator will consult with a more senior manager within the service or, where appropriate, with a manager from another service or Portfolio. 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. To ensure that your concern is dealt with efficiently and appropriately it is important that the right process is followed. If the Whistleblowing Co-ordinator considers that the concern falls within the scope of another procedure, such as the Grievance Procedure or Dignity and Respect, they will tell you and advise that it is referred to the relevant manager for appropriate action. This does not mean that your concern is not taken seriously but that it can be addressed more effectively using another procedure. 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.

The verification of your complaint should take place within 10 working days of you raising it.

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

In consultation with the appropriate service manager or Director, the Whistleblowing Co-ordinator will identify an investigating officer or team. Where managers or Directors within the service may be the subject of the allegations then the Whistleblowing Co-ordinator will consult with a more senior manager within the service or, where appropriate, with a manager from another service or Portfolio, the Monitoring Officer or the Chief Executive.

The investigating officer or team will be supported by a HR Advisor.

The Whistleblowing Co-ordinator and the service manager or Director will jointly commission the investigation.

The Investigating Officer will 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 however we aim to conclude whistleblowing investigations within 12 weeks wherever possible. You will be informed if this is not achievable and you will also be advised when the investigation is concluded.

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 with the reasonable belief that the person disclosed information in the public interest.

The report will be presented to and considered by the Whistleblowing Co-ordinator and the commissioning manager or Director. The commissioning manager or Director will be responsible for implementing agreed recommendations with the support of the Whistleblowing Co-ordinator or HR where appropriate. A clear and reasonable timescale should be set for implementing the recommendations which shouldn't exceed three months.

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.

As this procedure is aimed at raising concerns where the interests of others or the organisation may be at risk, the person raising the complaint will not normally receive the report. Where legal and confidentiality constraints allow, you will receive information about the outcome of any investigation. This may include findings and recommendations.

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 quarterly basis to the Monitoring Officer who provides reports as necessary to the Standards Committee. The Monitoring Officer will be updated on a regular basis where cases are investigated.

Legal changes incorporated which take effect from 25 June 2013. Policy updated October 2013

Appendix A

ROLES AND RESPONSIBILITIES

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 quarterly 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.

Contact Advisors

The Contact Advisors 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 Contact Advisors 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 where this is requested by the person raising the complaint
- Completing reporting requirements

The Contact Advisors are trained to handle situations and individuals sensitively, fairly and promptly and to maintain confidentiality wherever possible.

Whistleblowing Co-ordinators

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 Contact Advisors 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 in consultation with the commissioning manager or Director
- 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

Human Resources

The Human Resources Team are responsible for:

- Development and maintenance of the policy
- Communicating and publicising the policy
- Maintaining the list of Contact Advisors and Co-ordinators and ensuring that appropriate briefing and training is provided
- Provide advice to managers on the appropriate procedure for concerns raised initially under this procedure
- Supporting investigations

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

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 reports on finance or fraud related issues raised through the whistleblowing 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 and to be informed about implications for conduct and ethics within the Council.

~~**APPENDIX D**~~

~~**October 2012**~~

~~**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 roof 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. If you are complaining that you have suffered harassment, discrimination, victimisation or bullying at work please use the Dignity and Respect Procedure which is on the intranet. If, however, your concern is about the dignity and respect of others then it may be appropriate to use this procedure. 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.

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.

Information and support

The Council has a number of Contact Advisors who can provide advice and information to help you explore the appropriate routes to raise your concern. The Contact Advisors can also provide support as the investigation progresses.

If you are a member of a recognised Trade Union your Trade Union can also support you.

Your right to support in meetings
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.

The meetings you may be required to attend are:

- 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 or the Dignity and Respect 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 IF YOU ARE THE SUBJECT OF A COMPLAINT UNDER THIS POLICY

If you are the subject of a complaint under this policy and procedure you have the right to be accompanied by your Trade Union Representative or a work colleague at any meetings relating to the complaint but this should not be your line manager as they may be required to implement any recommendations that come out of the investigation.

The Council's Contact Advisors can provide support and guidance about the whistleblowing procedure and investigations to both parties. You can access that support if you have whistleblowing allegations raised against you.

If you are the subject of a complaint or investigation under this policy your confidentiality will be respected as with any other procedure.

1.6 INDEPENDENT ADVICE

If you are unsure whether to use this policy or you want independent advice at any stage, you may contact:

- A Whistleblowing Contact – contact details are provide in Appendix C or on the intranet
- 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.

1.7 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, e.g.~~
    - ~~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.~~

~~1.8 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.~~

~~If you are unhappy with the way you are treated when raising your concern or during the investigation, you can raise this under the Grievance Procedure or under the Dignity and Respect procedure as appropriate but you should not use these alternative procedures to raise the same issues that you raised in your original whistleblowing complaint.~~

~~SECTION 2 – RAISING A WHISTLEBLOWING CONCERN~~

~~2.1 WHAT TYPES OF CONCERNS CAN BE RAISED~~

~~You can use the Whistleblowing Policy to raise concerns about something, involving employees, 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 Standards Committee, in a form that will maintain your confidentiality as far as possible. The Monitoring Officer may delegate this responsibility to the Deputy Monitoring Officer. 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 or a complaint about dignity and respect, rather than a whistleblowing matter, we will tell you.

You or your trade union representative on your behalf 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 (for example, they may be involved in the issue that you are concerned about), you could raise it with a more senior manager in your service or you can use one of the alternative options below.~~

~~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.~~

~~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.~~

~~c) Raise it directly with a Whistleblowing Co-ordinator~~

~~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 who will allocate it to an appropriate Whistleblowing Co-ordinator.~~

~~d) Raise it with the Council's Monitoring Officer~~

~~If you feel the matter is so serious that you cannot discuss it with any of the officers set out above you can raise it with the Council's Monitoring Officer who will allocate it to an appropriate Whistleblowing Co-ordinator.~~

~~Concerns can be raised verbally, by arranging a meeting with the appropriate officer, or in writing by letter or email.~~

~~e) 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.*~~

f) 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.

Your right to support in meetings

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.

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 in consultation with the appropriate service manager or Director. Where managers or Directors within the service may be the subject of the allegations then the Whistleblowing Co-ordinator will consult with a more senior manager within the service or, where appropriate, with a manager from another service or Portfolio. 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. To ensure that your

~~concern is dealt with efficiently and appropriately it is important that the right process is followed. If the Whistleblowing Co-ordinator considers that the concern falls within the scope of another procedure, such as the Grievance Procedure or Dignity and Respect, they will tell you and advise that it is referred to the relevant manager for appropriate action. This does not mean that your concern is not taken seriously but that it can be addressed more effectively using another procedure. 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.~~

~~The verification of your complaint should take place within 10 working days of you raising it.~~

~~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~~

~~In consultation with the appropriate service manager or Director, the Whistleblowing Co-ordinator will identify an investigating officer or team. Where managers or Directors within the service may be the subject of the allegations then the Whistleblowing Co-ordinator will consult with a more senior manager within the service or, where appropriate, with a manager from another service or Portfolio, the Monitoring Officer or the Chief Executive.~~

~~The investigating officer or team will be supported by a HR Advisor.~~

~~The Whistleblowing Co-ordinator and the service manager or Director will jointly commission the investigation.~~

~~The Investigating Officer will 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 however~~

we aim to conclude whistleblowing investigations within 12 weeks wherever possible. You will be informed if this is not achievable and you will also be advised when the investigation is concluded.

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 be presented to and considered by the Whistleblowing Co-ordinator and the commissioning manager or Director. The commissioning manager or Director will be responsible for implementing agreed recommendations with the support of the Whistleblowing Co-ordinator or HR where appropriate. A clear and reasonable timescale should be set for implementing the recommendations which shouldn't exceed three months.

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.

As this procedure is aimed at raising concerns where the interests of others or the organisation may be at risk, the person raising the complaint will not normally receive the report. Where legal and confidentiality constraints allow, you will receive information about the outcome of any investigation. This may include findings and recommendations.

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 quarterly basis to the Monitoring Officer who provides reports as necessary to the Standards Committee. The Monitoring Officer will be updated on a regular basis where cases are investigated.

~~Revised October 2012~~

~~Appendix A~~

~~ROLES AND RESPONSIBILITIES~~

~~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 quarterly 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.~~

~~Contact Advisors~~

~~The Contact Advisors 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 Contact Advisors 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 Contact Advisors are trained to handle situations and individuals sensitively, fairly and promptly and to maintain confidentiality wherever possible.~~

~~Whistleblowing Co-ordinators~~

~~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 Contact Advisors 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 in consultation with the commissioning manager or Director~~
- ~~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~~

~~Human Resources~~

~~The Human Resources Team are responsible for:~~

- ~~Development and maintenance of the policy~~
- ~~Communicating and publicising the policy~~
- ~~Maintaining the list of Contact Advisors and Co-ordinators and ensuring that appropriate briefing and training is provided~~
- ~~Provide advice to managers on the appropriate procedure for concerns raised initially under this procedure~~
- ~~Supporting investigations~~

~~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~~

~~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 reports on finance or fraud related issues raised through the whistleblowing 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 and to be informed about implications for conduct and ethics within the Council.~~

~~Appendix B~~

~~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~~

~~Appendix C~~

~~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.~~

~~James Henderson~~	~~Director of Policy, Performance & Communications~~	~~2753126~~
~~Chris Shaw~~	~~Director of Health Improvement~~	~~2735015~~
~~Lynne Bird~~	~~Director of Legal & Governance~~	~~2734018~~
~~Eugene Walker~~	~~Director of Finance~~	~~2735872~~
~~Julie Toner~~	~~Director of Human Resources~~	~~2734081~~
~~Cheryl Blackett~~	~~Head of Human Resources, Specialist & Advisory Services~~	~~2734080~~
~~Sue Palfreyman~~	~~Head of Human Resources, Business Systems, Capability, Development & Change~~	~~2735530~~
~~Nalin Seneviratne~~	~~Director of Capital & Major Projects~~	~~2057017~~
~~Paul Green~~	~~Director of Business Information and Transformation~~	~~2736818~~
~~Barry Mellor~~	~~Director of Commercial Services~~	~~2053928~~
~~Julie Bullen~~	~~Director of Customer Services~~	~~2736972~~
~~Neil Dawson~~	~~Director of Transport & Facilities Management~~	~~2037592~~
~~Jayne Ludlam~~	~~Interim Director of Children, Young People & Families~~	~~2735726~~
~~Matthew Sampson~~	~~Acting Deputy Executive Director CYPF~~	~~2734913~~
~~John Doyle~~	~~Director of Business Strategy~~	~~2735663~~
~~Maggie Williams~~	~~Deputy Executive Director CYPF~~	~~2930968~~
~~Tony Tweedy~~	~~Director of Lifelong Learning, Skills & Communities~~	~~2296140~~
~~Edward Highfield~~	~~Director of Creative Sheffield~~	~~2232349~~
~~Paul Billington~~	~~Director of Culture and Environment~~	~~2734700~~
~~Les Sturch~~	~~Director of Regeneration & Development Services~~	~~2735449~~
~~Mick Crofts~~	~~Director of Business Strategy & Regulation~~	~~2735776~~
~~Andy Nolan~~	~~Lead - Sustainable Cities Programme~~	~~2057415~~
~~Eddie Sherwood~~	~~Director of Care and Support Communities~~	~~2734840~~
~~Joe Fowler~~	~~Director of Commissioning~~	~~2734605~~
~~Jan Fitzgerald~~	~~Interim Director of Community Services~~	~~2734486~~
~~Bev Coukham~~	~~Director of Business Strategy~~	~~2053105~~
~~Janet Sharpe~~	~~Interim Director of Housing~~	~~2735074~~

~~WHISTLEBLOWING CO-ORDINATORS~~

~~Human Resources~~		
~~Cheryl Blackett~~	~~Head of Human Resources, Policy and Governance~~	~~2734080~~
~~Sue Palfreyman~~	~~Head of Human Resources, Service Delivery~~	~~2735530~~
~~Legal~~		
~~Lynne Bird~~	~~Director of Legal & Governance~~	~~2734018~~
~~Finance~~		
~~Eugene Walker~~	~~Director of Finance~~	~~2735872~~
~~Health and Safety~~		
~~Steve Clark~~	~~HR Manager~~	~~2734796~~
~~Safeguarding~~		
~~Cath Erine~~	~~Service Manager~~	~~2736870~~
~~Karen Bennett~~	~~Service Manager~~	~~2053846~~
~~Des Charles~~	~~Service Manager~~	~~2735819~~
~~Audit~~		
~~Fraud Hotline~~		~~2736060~~

~~TRADE UNION REPRESENTATIVES~~

~~Jon Mordecai~~	~~UNISON~~	~~2736307~~
~~Mark Keeling~~	~~UNITE~~	~~2736486~~
~~Shelagh Carter~~	~~GMB~~	~~2768017~~

~~CONTACT ADVISERS~~

~~Marjorie Fee~~	~~07989 359564~~
~~Gary Dickson~~	~~07803 888493~~
~~Satya Thompson~~	~~07876 038745~~
~~Tracey Jack~~	~~07785 294106~~
~~Fiona Sinclair~~	~~07799 342583~~
~~Karen Ramsay~~	~~07768 698577~~
~~Fayzeh Mohamed~~	~~07730 815657~~
~~Josie Billings~~	~~07785294639~~

~~(Contact Officers/Co-ordinators/Trade Union Representatives/Contact Advisers last updated June 2013)~~

APPENDIX E

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 V.~~Article IX. **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 VI.~~Article X.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 (e.g. 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 user's 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 user's 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

Sheffield City Council

Social Networking Policy

Publication Date: July 2013

Author: HR Specialist Services

Social Networking Policy

○ Purpose

It is very much in our (the Council's) interest to allow you (the employee) to participate in this rapidly growing environment of relationships, learning and collaboration.

This policy provides you with a set of principles for using social networking sites responsibly, which is linked to the Officers' Code of Conduct and associated policies. It gives you clear guidelines, so you can protect yourselves by complying with our conduct rules, with the laws on harassment, discrimination, data protection, copyright and ensuring your own safety.

The policy ensures that we are not exposed to financial, legal and governance risks and that the safeguarding of children, young people and vulnerable adults is not threatened by the use of social networking

As this is a new policy, which is to be used across the organisation and everybody is impacted by it, it is important that this is reviewed regularly, initially by Executive Management Team after 6 months.

2.0 Introduction

Sheffield City Council recognises that the internet provides unique opportunities to participate in interactive discussions and share information using a wide variety of social networking sites.

We believe in open exchange using social networking sites to empower you and customers. These individual interactions represent a new model: not mass communication but masses of communicators. Through these interactions, you and local people are empowered to learn, share your expertise and promote what is best in Sheffield.

- You can contribute best practice on our services - sharing your expertise, raising Sheffield's profile.
- Through individual interactions, you can better involve and engage with a wider range of people, including young people and people setting up new businesses in the city. This allows us to learn from our customers, drawing on their expertise and knowledge to design services that meet their needs.
- By encouraging local people to contact us using social networking sites – e.g. via e-petitions - we can gain information on key issues to help inform policy in the city.
- Use social networking as a technology platform for open innovation and learning, which makes it easier for you to learn, develop, reflect on practice, be creative and collaborate for improved services.

Whilst we have embraced these technological innovations as part of our working and private lives, employers are now grappling with consequences of unacceptable posts, which are rapid communicated and shared. We have recently dealt with social networking issues relating to:-

- Bullying and harassment,
- Freedom of expression of political views
- private/professional boundaries with children
- problems with blurring private/professional boundaries – manager/employee
- work-related offensive photos
- being off sick and using social networking for secondary employment
- Employee petition against service closures.

In many of these cases, the employees were unaware that social networking is not private and that there are potential consequences to their on-line activity.

Managers, Trade Union Representatives and HR Practitioners have therefore asked for helpful, practical advice to protect you and us, when you use social networking sites in a work and private capacity. Representatives from all these groups, plus Members of the Equality Forums have contributed to this policy.

3.0 Scope

This policy applies to all non-schools based Sheffield City Council employees, casual workers, agency staff, contractors, consultants, self-employed people, apprentices, trainees and those on work placements, who work for the Council. Throughout this policy, the term 'employee' and 'you' is used to cover all these types of workers. The Social Media Policy adopted by the relevant Governing Body will apply to teaching and support staff in schools.

This policy deals with the use of all forms of social networking including but not limited to Twitter, MySpace, Facebook, texts, emails, BlackBerry Messenger (BBM), LinkedIn, Blogs, Wikipedia sites and any other sites which involve document, photo or video sharing such as YouTube or new networks, internet sites/channels that may be developed in the future.

This policy applies to the use of social networking for both work and personal purposes, whether during working hours or otherwise and whether at work or elsewhere including in your home. It also applies regardless of whether the social networking site is accessed using our ICT facilities/equipment or that belonging to you.

This policy should be read in conjunction with:

- Officers' Code of Conduct and associated policies
  - Member-Officer Relations Protocol
  - Information Security Policy and e-communications guidance
  - Dignity and Respect at Work Policy

- Social Networking Guidance
- Draft Safeguarding Children and Vulnerable Adults Policy
- Disciplinary Procedure
- Recruitment and Selection Policy
- Social Media Position Statement, EMT (June 2011)

Responsibilities

The Council

We recognise the benefits of social networking and trust you to act responsibly. We expect you to work in the same way on-line and off-line, following the behaviours set out in the Officer Code of Conduct, as detailed in this policy and in associated guidance.

We permit personal use of social networking sites at work during break times as long as it is not excessive and/or does not involve unprofessional or inappropriate conduct and does not interfere with your responsibilities or performance. You need to bear in mind that you must take short breaks away from screens to protect your health.

We also know that some employees and their managers need to consider safety of their service users and themselves, if they use social networking sites. These sites are public and there is a possibility that employees or service users could be traced, resulting in harm to that person. Where this is an issue, employees and their manager will need to carry out a risk assessment for using social networking for work purposes.

Employees

You are personally responsible for the content you publish on-line and must be mindful that **everything placed on-line is public** and is hard to remove once posted.

You should follow our social networking principles, which are divided into 4 themes, with the core behaviours applying across the themes.
In brief, you should:-

- Be professional when using social networking for work and personal use
- Be respectful at all times, never post offensive or intimidating texts or images about a person
- Familiarise yourself with this social networking policy and associated guidance

You are responsible for the success of this policy and should ensure that you take the time to read and understand it. You should report any misuse of social networking to the appropriate line manager.

Managers

All managers have a specific responsibility for operating within the boundaries of this policy. You must ensure that your employees understand the standards of behaviour expected of them and take action if behaviour falls below the required standard.

Managers should:

- Familiarise themselves with the Social Networking Policy and guidelines
- Ensure their staff are aware of the policy
- Take prompt action to stop any harassment or bullying they become aware of, whether a complaint has been raised or not
- Support the staff involved in any allegations about cyber bullying, harassment, discrimination, using existing procedures
- Ensure all complaints/allegations are dealt with fairly and consistently and in line with other employment policies.

HR and Trade Unions should

Provide support and advice to managers and employees on the operation of the policy and guidelines, where necessary.

Compliance

You must comply with Council policies and the law when using social networking sites. Make sure that you:-

- Know and comply with the Officers' Code of Conduct and associated policies including the Dignity and Respect Policy, Information Security Policy and E-Communications Guidance.

- Only share public information on-line. Information that is not public, such as service user, employee or manager information given in confidence, may only be shared in accordance with the law. If you use non-public information inappropriately, you may be personally prosecuted under the Data Protection Act.

- Are professional, when posting comments about the Council and our services. Be aware that the Council may take disciplinary action, if there is a reasonable belief that your on-line comments have damaged the Council's reputation.

- Are respectful at all times to our customers and colleagues. Never post offensive or intimidating texts or images about a person.

You are expected to use the **same professional behaviours on-line,** as you would when communicating with service users and colleagues **off-line.** You must not post any information or messages on-line, that you would be unwilling to say in public face to face. Make sure that you follow the principles and standards set out in this policy, in the Officer Code of Conduct and associated listed policies.

Where your manager identifies that you may have fallen short of the standards in this policy, your manager is to deal with the matter informally where appropriate. The formal procedure will be used however, to guide you towards achieving acceptable standards as set out in this policy. You may have disciplinary action taken against you, if you do not keep to this policy, which includes the possibility of being dismissed without notice being given. Serious breaches of this policy for example incidents of bullying on social networking sites may constitute gross misconduct and dismissal.

Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. You are required to co-operate with investigations into allegations made under this policy.

You must not make false or malicious allegations about another person's use of social networking and need to be aware that disciplinary action may be considered in such circumstances.

You may be required to remove social networking posts, which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Social Networking Principles

Personal Use

1. Be professional, know and follow the Officer Code of Conduct. You are personally responsible for what you post. Be thoughtful about how you present yourself in social networks. Understand that social networking is a public forum and your entries are not private and are hard to remove once posted.

2. We can ask you to remove on-line content if we have a reasonable belief that it is damaging the Council's reputation. If we can prove that your conduct on-line has caused detriment, you may face disciplinary action and if severe enough, you could be dismissed as a result.

3. You have a right to express political and religious views, as long as they are lawful, are made in a private capacity and do not impact on your job. Some employees are in politically restricted posts and need to maintain political impartiality.

4. Do raise any work-related concerns in the right way. You can speak to your manager, give feedback in the employee survey, attend staff forums, speak to a contact advisor, contact your trade union representative, get support from the independent employee assistance programme or for serious allegations, use the whistle-blowing procedure. This allows us to investigate and address the issue in the first instance.

5. As you are an employee of the Council, you must ensure that your on-line content is consistent with your professional image that you present for the Council.

6. Be respectful of other employees, service users or customers as set out in our Dignity and Respect at Work Policy.

7. There is no expectation for you to accept 'friend' requests from colleagues or managers

8. You are allowed appropriate and reasonable personal use of social networking at work, using Council or your own equipment. This is to take place in your own time and outside core hours, not adversely affecting performance or provision of service. Personal use of Council equipment is at no additional cost to the Council.

Business Use

9. When acting on behalf of the organisation, you must be professional. Always be responsible for your on-line comments, be credible, accurate and fair. Make sure that you are respectful at all times, especially when replying to disagreements. Avoid unnecessary or unproductive arguments. Do not speculate about an issue or start inflammatory debates. Make sure what you say is factually correct.

10. If you have any doubts about content, do not post without escalating to a manager. If you make an error, be up front about your mistake and correct it quickly, as this can help to restore trust. If your mistake is serious, let your manager know immediately and get advice. Ultimately, you are responsible for what you post or publish on a social networking site.

Maintaining Professional Relationships

11. You have a specific duty of care to take reasonable steps to protect service users, colleagues and yourself from harm. You must discuss any safety issues of using social networking sites for work purposes with your manager and if relevant draw up a risk assessment. This may state that you must only use secure forms of communications for work purposes. If you receive a serious on-line threat to life or buildings, you must contact the police immediately and let your manager know.

12. If you are in a **position of trust** with **Children** or **Vulnerable Adults**, for example if you work in social care, you have a professional relationship with your service users. You must draw a line between your professional and private life.

    You must not strike up or accept an on-line relationship with your service users, using a personal social networking account. This applies even if your service users are no longer receiving a service.

    Similar to your off-line work, where you have a close relationship with a service user, you must let your manager know. You must declare any interest you may have with a person, which may cause a direct or indirect conflict of interest with your employment. This information is provided to protect you and service users against any allegation of favour or disadvantage.

13. If you interact with **Elected Members** on social networking sites, you must follow the existing rules within Officers' Code of Conduct and Member-Officer Relations Protocol. Officers in politically restricted posts must be particularly carefully to be impartial and maintain professional relationships.

Gathering and Sending Out Information

14. You can provide any Council Public Information to social networking sites. This is information, which is already in the public domain. You must keep non-public information secure and never release this to social networking sites. Non-Public Information includes personal data about service users or employees. If you suspect that any of your social networking accounts have been hacked, resulting in an impact on your work, you must let your manager know immediately.

15. Any monitoring or surveillance of a customer or employee is strictly controlled and you must be authorised to carry out this activity. For example, you must never become a 'friend' of any service user or employee for the purpose of obtaining information, unless authorised.

16. We reserve the right to monitor your social networking and internet use at work. Valid reasons for checking your usage include suspicions that you have:

    - Been spending an excessive amount of time viewing sites that are not work-related or
    - Acted in a way that damages the reputation of the Council and/or breaches disclosure of non-public information

APPENDIX GF

(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 HG

Politically Restricted Posts (PoRPs) (Revised May 2012/Minor Amendment February 2013)

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 (Director of Legal and Governance)

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 (Director of Legal and Governance), 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 ~~I~~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 person's 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:

Dignity and Respect Procedure – this should be used if they feel they have experienced harassment, discrimination, victimisation or bullying at work by another Council employee.
Grievance Procedure – this should be used if an employee wants to raise significant and specific concerns about their employment or treatment at work.
Accident, Violent Incident or Near Miss Report Form 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.
Whistleblowing Procedure - 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.

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.