Public Document Pack

Audit and Standards Committee

Thursday 19 October 2023 at 5.00 pm

Town Hall, Sheffield, S1 2HH

The Press and Public are Welcome to Attend

Membership

Councillors Mohammed Mahroof (Chair), Sioned-Mair Richards (Deputy Chair), Sue Alston, Fran Belbin, Simon Clement-Jones, Laura McClean and Henry Nottage.

Independent Co-opted Members

Alison Howard.

Sheffield
City Council

PUBLIC ACCESS TO THE MEETING

The Audit and Standards Committee oversees and assesses the Council's risk management, control and corporate governance arrangements and advises the Council on the adequacy and effectiveness of these arrangements. The Committee has delegated powers to approve the Council's Statement of Accounts and consider the Annual Letter from the External Auditor.

The Committee is also responsible for promoting high standards of conduct by Councillors and co-opted members.

A copy of the agenda and reports is available on the Council's website at http://democracy.sheffield.gov.uk. You can also see the reports to be discussed at the meeting if you call at the First Point Reception, Town Hall, Pinstone Street entrance. The Reception is open between 9.00 am and 5.00 pm, Monday to Thursday and between 9.00 am and 4.45 pm. on Friday. You may not be allowed to see some reports because they contain confidential information.

Recording is allowed at meetings of the Committee under the direction of the Chair of the meeting. Please see the website or contact Democratic Services for details of the Council's protocol on audio/visual recording and photography at council meetings.

If you require any further information please contact Jay Bell in Democratic Services via email jay.bell@sheffield.gov.uk.

FACILITIES

There are public toilets available, with wheelchair access, on the ground floor of the Town Hall. Induction loop facilities are available in meeting rooms.

Access for people with mobility difficulties can be obtained through the ramp on the side to the main Town Hall entrance.

AUDIT AND STANDARDS COMMITTEE AGENDA
19 OCTOBER 2023

Order of Business

1. **Welcome and Housekeeping Arrangements**

2. **Apologies for Absence**

3. **Exclusion of the Press and Public**
To identify items where resolutions may be moved to exclude the press and public.

4. **Declarations of Interest** (Pages 5 - 8)
Members to declare any interests they have in the business to be considered at the meeting.

5. **Minutes of Previous Meeting** (To Follow)
To approve the minutes of the meeting of the Committee held on 21 September 2023

6. **Public Questions and Petitions**
To receive any questions or petitions from members of the public

7. **Information Management Annual Report** (Pages 9 - 24)
Report of the Chief Operating Officer

8. **Information Commissioner's Office (ICO) FOI Audit Report** (Pages 25 - 36)
Report of the Chief Operating Officer

9. **Work Programme** (Pages 37 - 46)
Report of the General Counsel

10. **Dates of Future Meetings**
To note that the next meeting of the Committee will be held at 5.00 p.m. on 23 November 2023

This page is intentionally left blank

ADVICE TO MEMBERS ON DECLARING INTERESTS AT MEETINGS

If you are present at a meeting of the Council, of its Policy Committees, or of any committee, sub-committee, joint committee, or joint sub-committee of the authority, and you have a **Disclosable Pecuniary Interest** (DPI) relating to any business that will be considered at the meeting, you must not:

- participate in any discussion of the business at the meeting, or if you become aware of your Disclosable Pecuniary Interest during the meeting, participate further in any discussion of the business, or
- participate in any vote or further vote taken on the matter at the meeting.

These prohibitions apply to any form of participation, including speaking as a member of the public.

You **must**:

- leave the room (in accordance with the Members' Code of Conduct)
- make a verbal declaration of the existence and nature of any DPI at any meeting at which you are present at which an item of business which affects or relates to the subject matter of that interest is under consideration, at or before the consideration of the item of business or as soon as the interest becomes apparent.
- declare it to the meeting and notify the Council's Monitoring Officer within 28 days, if the DPI is not already registered.

If you have any of the following pecuniary interests, they are your **disclosable pecuniary interests** under the new national rules. You have a pecuniary interest if you, or your spouse or civil partner, have a pecuniary interest.

- Any employment, office, trade, profession or vocation carried on for profit or gain, which you, or your spouse or civil partner undertakes.

- Any payment or provision of any other financial benefit (other than from your council or authority) made or provided within the relevant period* in respect of any expenses incurred by you in carrying out duties as a member, or towards your election expenses. This includes any payment or financial benefit from a trade union within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992.

  *The relevant period is the 12 months ending on the day when you tell the Monitoring Officer about your disclosable pecuniary interests.

- Any contract which is made between you, or your spouse or your civil partner (or a body in which you, or your spouse or your civil partner, has a beneficial interest) and your council or authority –

  - under which goods or services are to be provided or works are to be executed; and
  - which has not been fully discharged.

- Any beneficial interest in land which you, or your spouse or your civil partner, have and which is within the area of your council or authority.

- Any licence (alone or jointly with others) which you, or your spouse or your civil partner, holds to occupy land in the area of your council or authority for a month or longer.

- Any tenancy where (to your knowledge) –
  - the landlord is your council or authority; and
  - the tenant is a body in which you, or your spouse or your civil partner, has a beneficial interest.

- Any beneficial interest which you, or your spouse or your civil partner has in securities of a body where -

  (a) that body (to your knowledge) has a place of business or land in the area of your council or authority; and

  (b) either -
    - the total nominal value of the securities exceeds £25,000 or one hundredth of the total issued share capital of that body; or
    - if the share capital of that body is of more than one class, the total nominal value of the shares of any one class in which you, or your spouse or your civil partner, has a beneficial interest exceeds one hundredth of the total issued share capital of that class.

If you attend a meeting at which any item of business is to be considered and you are aware that you have a **personal interest** in the matter which does not amount to a DPI, you must make verbal declaration of the existence and nature of that interest at or before the consideration of the item of business or as soon as the interest becomes apparent. You should leave the room if your continued presence is incompatible with the 7 Principles of Public Life (selflessness; integrity; objectivity; accountability; openness; honesty; and leadership).

You have a personal interest where –

- a decision in relation to that business might reasonably be regarded as affecting the well-being or financial standing (including interests in land and easements over land) of you or a member of your family or a person or an organisation with whom you have a close association to a greater extent than it would affect the majority of the Council Tax payers, ratepayers or inhabitants of the ward or electoral area for which you have been elected or otherwise of the Authority's administrative area, or

- it relates to or is likely to affect any of the interests that are defined as DPIs but are in respect of a member of your family (other than a partner) or a person with whom you have a close association.

Guidance on declarations of interest, incorporating regulations published by the Government in relation to Disclosable Pecuniary Interests, has been circulated to you previously.

You should identify any potential interest you may have relating to business to be considered at the meeting. This will help you and anyone that you ask for advice to fully consider all the circumstances before deciding what action you should take.

In certain circumstances the Council may grant a **dispensation** to permit a Member to take part in the business of the Authority even if the member has a Disclosable Pecuniary Interest relating to that business.

To obtain a dispensation, you must write to the Monitoring Officer at least 48 hours before the meeting in question, explaining why a dispensation is sought and desirable, and specifying the period of time for which it is sought. The Monitoring Officer may consult with the Independent Person or the Council's Standards Committee in relation to a request for dispensation.

Further advice can be obtained from David Hollis, General Counsel by emailing david.hollis@sheffield.gov.uk.

This page is intentionally left blank

Audit and Standards Committee Report

Report of:	**Chief Operating Officer**
Date:	**09/10/2023**
Subject:	**Information Governance Annual Report**
Author of Report:	**Sarah Green** **Senior Information Management Officer and Data Protection Officer**

Summary:

Information Governance is the generic term used to describe how an organisation manages its information, particularly in respect to legislative and regulatory requirements. This report seeks to provide assurance around the policies, processes and practices employed to ensure that we meet those requirements.

Recommendations: To note the annual information governance update

Background Papers: None

Category of Report: OPEN

Statutory and Council Policy Checklist

Financial Implications
NO
Legal Implications
YES
Equality of Opportunity Implications
NO
Tackling Health Inequalities Implications
NO
Human rights Implications
NO
Environmental and Sustainability implications
NO
Economic impact
NO
Community safety implications
NO
Human resources implications
NO
Property implications
NO
Area(s) affected
None
Relevant Cabinet Portfolio Member
Councillor Cate McDonald
Is the item a matter which is reserved for approval by the City Council?
NO
Press release
NO

REPORT TITLE: Information Governance Annual Report for 2022/23

1.0 INTRODUCTION

1.1 This report has been written to provide an overview of the Information Governance arrangements and performance at the Council for the last financial year, and to provide assurance around the policies, processes and practices employed to ensure that we meet our legal requirements.

It is important to note that this is a retrospective report, covering the financial year 2022/23.

2.0 BACKGROUND

2.1 Information Governance is a common term for the distinct, but overlapping, disciplines of data protection; access to information, information security; investigatory powers; information and records management; information sharing; data quality and information assurance.

2.2 The ultimate purpose of Information Governance is to help an organisation to understand its information needs and responsibilities; to define the rules for the management of information flowing in, out and around the business, and to maximise the value of information while minimising the risks.

2.3 Effective Information Governance enables the Council to understand and comply with its legal and administrative obligations; manage, and reduce risks; protect privacy and confidentiality, and support services to deliver to the right people at the right time.

2.4 The Information Governance landscape is complex and subject to laws, regulations, and recommended codes of practice. The key laws include the General Data Protection Regulation 2016/679 (GDPR), which since Brexit has become the UK GDPR; Data Protection Act 2018 (DPA); Freedom of Information Act 2000 (FOIA); Environmental Information Regulations 2004 (EIR), and Regulation of Investigatory Powers Act 2000 (RIPA). The Council can be called upon to demonstrate its compliance with these laws and regulations by members of the public, partner agencies, accrediting bodies, and regulators such as the Information Commissioner’s Office (ICO), the Biometrics and Surveillance Camera Commissioner, and the Investigatory Powers Commissioner. These commissioners have powers to impose penalties, including monetary penalties and custodial sentences, on organisations or individuals who breach the laws and regulations.

2.5	To enable the Council to understand and shape Information Governance activity across the organisation and ensure compliance, it has nominated specific information governance roles to officers: Senior Information Risk Owner, Portfolio Information Risk Owners, Caldicott Guardians, Senior Responsible Officer (RIPA), Senior Responsible Officer (CCTV) and the Data Protection Officer. These roles attend the Information Governance Board, which is subsequently supported by key officers and working groups to help embed information governance practice. In 2019/20, the Council nominated its directors to become Information Asset Owners and gave them responsibility for managing risks to the personal data and business critical information held within their services.
3.0	**DATA PROTECTION LAWS**
3.1	2022/23 was the fifth financial year in which the General Data Protection Regulation (GDPR) 2016/679 (now the UK GDPR) and the Data Protection Act (DPA) 2018 have been in force. The Council has continued to work to ensure compliance with the law and an ongoing GDPR Action Plan is in place.
3.2	Where 2017-19 had been spent preparing for GDPR, 2019/20 adapting to the new law, 2020/22 were the years of the pandemic. The government began to prepare for a shake-up of UK data protection law with a consultation in September 2021 called “Data: a new direction”. This Bill was withdrawn on 8th March 2023 and a new bill introduced to Parliament, The Data Protection and Digital Information (No.2) Bill. This is currently at Report stage with Parliament. In January 2022, John Edwards, took up his post as the sixth Information Commissioner since the Data Protection Act 1984. The Council has continued to work to ensure compliance with the law and an ongoing GDPR Action Plan is in place.
3.3	Data protection compliance remains a key priority for the Council and is currently logged on the Council’s Risk Register (Resources Risk ID 352 – High). Work will continue throughout 2023/24 to ensure good practice is understood and embedded into business as usual, and that proper governance is available as and when required to reduce the risk to an acceptable level.
4.0	**SUBJECT ACCESS REQUESTS**
4.1	Data protection law provides data subjects with a number of rights to better understand and make decisions about the personal data a Data Controller processes about them (Articles 14-22 GDPR). The most commonly exercised right is Article 15, the right of access, which is usually known as a Subject Access Request (SAR).

4.2 All SARs are logged by the Council’s Information Management Team, triaged, and allocated to individual services to provide a response.

4.3 SARs must be answered within a legal time limit – one calendar month, or three calendar months if a request is ‘complex’. The Council’s Information Governance Board has set the target that 90% of SARs should be answered on time.

4.4 In 2022/23, the Council handled 809 Subject Access Requests. 294 were withdrawn or abandoned by the customer and 515 were actioned. 338 of these were answered in time (see Appendix B). The overall SAR performance figure for 2022/23 is 65.6%.

4.5 The ICO has corresponded with the Council concerning fourteen separate complaints by data subjects about their Subject Access Requests in 2022/23. The majority of these cases concerned situations where individuals had complained to the ICO because they had not been provided with the information they had requested within the statutory timeframe. On two occasions, the ICO agreed that we had correctly refused requests as manifestly unfounded/excessive.

4.6 The handling of SARs remains a priority for the Council, in particular responding to information requests within the statutory timeframe.

5.0 FREEDOM OF INFORMATION (FOI) AND ENVIRONMENTAL INFORMATION (EIR) REQUESTS

5.1 The Council is legally required to respond to requests for information under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR). Responses must be made within 20 working days, subject to some exceptions. Each response must confirm if the information is held and then either provide the information or explain the reasons why it cannot be disclosed (exemptions/exceptions).

5.2 FOI and EIR requests are logged by the Council’s Information Management (IM) Team and then triaged and allocated to individual services to gather the information. Services provide a response to the IM Team, who check this, advise on the application of any exemptions/exceptions, and then respond to the customer.

5.3 In 2022/23, the Council received 1586 requests and answered 82.12% in time (Appendix A). This is a decrease on the number of information requests received in 2021/22, of 112 requests. The response rate is an improvement on the 76.22% achieved in 2020/21 but fails to meet the Information Governance Board’s target of 95% of requests answered in time. The ICO sets the acceptable compliance rate at 90%.

5.4 The six percent improvement in the compliance rate is in line with the return to normal working after the pandemic.

5.5 The FOI and EIR give a requester the right to appeal about the way their request has been handled. This is known as an Internal Review. The Council completed 37 Internal Reviews in 2022/23 (there was a backlog) of which eight related to responses in that year. In those cases, the Council upheld the complaint three times, and did not uphold the complaint five times.

Seven internal reviews remain outstanding from 2022/23 plus another nine from previous years.

5.6 In addition to the above, the Information Commissioner's Office has corresponded with the Council on 11 occasions concerning FOI/EIR requests received in 2022/23. Of these cases, three were because we were late with a response to the requester, which we subsequently provided. In the other eight cases, the ICO upheld one complaint by a requester, directing the council to disclose information. In the other seven cases, the ICO did not uphold requesters' complaints, and did not require the council to take any further steps.

6.0 OPEN DATA

6.1 Under the Freedom of Information Act 2000, Protection of Freedoms Act 2012, and the Local Transparency Code 2015, the Council is required to publish certain information on its website or open data sites. The Council is committed to open data to support its transparency agenda and routinely publishes information about its services, key decisions, and expenditure.

6.2 The risk relating to the publication of data on the Council's open data sites, including deciding what data should be published and ensuring that published data is accurate, meaningful, owned and regularly updated, remains logged on the Corporate Risk Register (Resources Risk ID 366 - Moderate).

6.3 In 2022/23, the Council has continued to work on improving its publication of open data, using Data Mill North to publish data relating to spend transparency, fleet vehicles, business rates and parking. To date 10 datasets have been published on Data Mill North. See: Search Datasets | Data Mill North

6.4 The Council also publishes 50 data sets of open data on the ARC GIS platform (ESRI) in 7 different categories, including environment, population, planning and transportation. See: Sheffield City Council Open Data (arcgis.com)

6.5 Further work is required to encourage services within organisation to recognise the benefits of open data to help demonstrate the Council's commitments to openness, transparency, and public accountability. This work will be reinvigorated following the reduction of pandemic backlogs.

7.0 INFORMATION SECURITY INCIDENTS AND PERSONAL DATA BREACHES

7.1 The Council is required to log, assess, and mitigate information security incidents and personal data breaches. Incidents can be events that have happened, or near misses that affect or are likely to affect the confidentiality, integrity, and availability of information. Where an incident occurs and affects personal data, this is a personal data breach. Data protection law requires organisations to notify the Information Commissioner's Office of personal data breaches that have a high and ongoing risk to the data subjects affected.

7.2 In 2022/23, 442 incidents were logged through the Council's information security incident process; 352 of these incidents were classed as personal data breaches (see Appendix C1). Most of these breaches involved customer personal data and were caused by human error with emails or post being delivered to the wrong person. Of these breaches, three were considered to meet the risk threshold and were reported to the Information Commissioner's Office. (see Appendix C2).

7.3 The Information Commissioner has the power to take enforcement action against an organisation for non-compliance with data protection law, which includes data breaches.

7.4 Incidents and data breaches have been reported by all Portfolios. The Services that handle sensitive personal data are at greater risk because an incident or breach is more likely to have a greater impact on the customer or data subject, and therefore meet the threshold to notify the Information Commissioner.

7.5 Consequently, there is a continuing and critical need to manage the information we have, safely and securely; to continue to implement sound data protection practice and to ensure all staff are aware of their responsibilities and have received and completed all the necessary training relevant to their role.

8.0 INVESTIGATORY POWERS COMMISSIONER

8.1 The Council is entitled to use the Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016 to carry out covert surveillance as part of its statutory duties. All applications must be approved by a Magistrate before covert surveillance can be carried out.

8.2 The Council must fully document all the applications it makes for covert surveillance, including the use of Covert Human Intelligence Sources, and make the documents available for inspection when required. The Council makes an annual return to the Investigatory Powers Commissioner’s Office, which confirms the number of applications that have been considered and submitted to a Magistrate (see appendix D).

8.3 In the calendar year 2022, the Council made 9 applications for Directed Surveillance (including renewals). These were for the statutory purpose of preventing or detecting crime or of preventing disorder.

8.4 The Investigatory Powers Commissioner (IPC) has the power to inspect an organisation to ensure its covert surveillance process and documentation is in place and compliant with the law. The Council received a desk-based and telephone inspection on 20 August 2020. The information provided has demonstrated a good level of compliance that removed, for the present, the requirement for a physical inspection. The IPC have changed their approach and no longer routinely undertake an inspection. Instead they will request a written report on compliance.

9.0 INFORMATION GOVERNANCE RISK AND ISSUES

9.1 In 2022/23, the Council maintained a number of Information Governance Risks and Issues on its Risk Register. These varied in severity – High to Low – covering compliance with UK GDPR, IT Transition and Cyber Security.

9.2 The risks are reported to the relevant senior managers every quarter – Senior Management Teams or the Executive Management Team – to ensure the risks are being progressed or to highlight any issues that affect the treatment plan.

10.0 INFORMATION SECURITY & CYBER SECURITY

10.1 Information security is about the protection of information or, more specifically, its confidentiality, integrity, and availability. The Council is required to take appropriate security measures to protect information, particularly personal data, from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to information transmitted, stored, or otherwise processed. This is increasingly including the protection of critical infrastructure, which is connected to the internet, or other networks, such as 4G or 5G.

10.2 Cyber security remains a constant threat and is recorded on the Council's asset register as such. Security experts consider that it is impossible to mitigate all cyber security threats and it is a case of when, rather than if, the Council is hit by a cyber-attack. This means that the Council’s approach must be to minimise the chances of a successful attack and be prepared to recover from any such an attack.

10.3 In addition, the National Cyber Security Centre has advised of significantly increased threat levels from potentially state backed organisations (in particular, following Russian’s invasion of Ukraine) and advised organisations to strengthen their security positions.

10.4 The move to hybrid working during and following the pandemic has also significantly changed the environment as the Council can no longer work on the basis that it only has to secure IT equipment located in corporate buildings over which is has full control., A large proportion of officers are now working at home or in non-council buildings.

10.5 The Council has invested heavily in Microsoft technology which support these new ways of working and provide strong security controls. Over this period, they have continued to roll out the security tools which are included in the investments we have made. In addition, we use Microsoft tools to regularly identify security risks and remediate vulnerabilities identified.

10.6 Additional security improvements over this period include moving most of the legacy and unsupported IT infrastructure onto supported infrastructure, and removing the significant threat of having out of date IT equipment across the estate.

10.7 The Council has moved its data to the Microsoft Azure platform, offering more resilient and faster backup solutions and strengthening our defences against the increasing threats of Ransomware attacks.

10.8 In addition to ongoing technical improvements, the Council have continued to work on its security policy framework to ensure we are aligned with industry standards such as ISO27001 and key compliance regimes including Payment Card Industry Data Security Standard (PCI-DSS) and the NHS Data Toolkit required for sharing data with the NHS.

10.9 We have worked during this period to improve our ability to proactively respond to threats through the implementation of Security Incident and Event Management (SIEM) and Security Orchestration and Automation and Response (SOAR) tools – as well as intrusion detection systems (IDS) to enable us to get early warnings of potential threats and incidents and take preventative action.

10.10 The security threat landscape and associated guidance and controls is forever changing and needs to be constantly monitored and kept under review. As part of the ongoing work, changes have been made or are in progress around the technical configuration of e-mail policy, administration toolsets and the management of privileged access as well as the development of updated IT Security and Acceptable Use policies.

11.0 RECORDS MANAGEMENT

11.1 Records Management is the practice of managing records with the intention of ensuring they are accurate, reliable, and available until they are disposed of or permanently preserved. Effective records management can underpin business practice, support decision making, and improve efficiencies, whereas ineffective records management can hinder operations and present a risk.

11.2 The Council continues to provide guidance, training, and awareness, explore better use of information technology to automate records management processes (especially retention and disposal), and gain a better understanding of management responsibility to own the information processed within their service area.

12.0 TRAINING

12.1 Information governance training is essential to ensure staff and other authorised users, or processers, of council information or systems understand and accept their responsibilities to handle information lawfully and safely. In the event of any complaint, incident or data breach, the Information Commissioner’s Office may ask for confirmation as to what training provision is in place and whether the employee involved in the matter has completed the training available.

12.2 The Council has a range of information governance related training, from general awareness courses to bespoke sessions on key topics. General training includes the Data Protection (GDPR) and Information Security e-learning and Regulation of Investigatory Powers e-learning, which were available thought the Sheffield Development Hub. Bespoke training has also been available and delivered to officers needing greater knowledge in key information governance areas, including data protection, data protection impact assessments, privacy notices and information sharing.

12.3 Information security training is mandatory. For our desk-based staff 96.1% had completed the learning and 38.6% of deskless staff had completed the learning. 95.35% of Social Care staff completed the training in time for the 2022/23 NHS Toolkit submission in June 2023.

12.4	Additionally, there has been training of discrete groups such as Foster Carers, student Social Workers, elected Members, Children and Families staff, ICT, comms and information governance for cyber-attacks, and intelligence sharing with the police. Staff have attended free webinars from solicitors’ firms, and national information governance trainers on data protection and Freedom of Information.

Appendix A: FOI and EIR Requests Response Performance 2022/23

	Requests Received	Responses Issued				
		Within 20 days	Overdue	Total	**% of Responses Issued which were issued within 20 days**	**% of Responses Issued which were overdue**
Quarter 1	420	285	49	334	**85.33%**	**14.67%**
Quarter 2	297	256	64	320	**80.00%**	**20.00%**
Quarter 3	324	233	65	298	**78.19%**	**21.81%**
Quarter 4	545	370	71	441	**83.90%**	**16.10%**
Full Year	**1586**	**1144**	**249**	**1393**	82.12%	17.88%

Appendix B-1: Subject Access Request Performance 20222/23

2022/23	Received	**Actioned**	Answered in time	Answered Late	**Compliance %**
Qtr 1	199	**130**	78	52	**60**
Qtr 2	186	**106**	61	45	**57.5**
Qtr 3	211	**139**	90	49	**64.7**
Qtr 4	213	**140**	109	31	**77.9**
Total	809	**515**	338	177	**65.6**

Year	Received	**Actioned**	Answered in time	Answered Late	**Compliance %**
2017/18	192	**192**	94	98	**49**
2018/19	297	**297**	219	78	**74**
2019/20	343	**343**	295	48	**86**
2020/21	326	**303**	170	133	**56**
2021/22	446	**366**	228	138	**62**

Appendix C: Reported Information Security Incidents and Personal Data Breaches

C-1 Quarterly Figures 2022-23

	No. of Incidents	ICO Notified
2022 -23		
Q1	**103**	**3**
Corruption or inability to recover information	1	0
Information disclosed in error (email, posted, fax, verbal)	82	3
Lost or stolen paperwork	2	0
Lost or stolen hardware	10	0
Online Disclosure (e.g. website, social media)	0	0
Unauthorised access to IT systems	3	0
Unauthorised access to physical documents	0	0
Cyber Attack	2	0
Non-secure disposal of paperwork	1	0
Other	2	0
Q2	**93**	**0**
Cyber Attack (e.g. virus, ransomware, phishing email)	1	0
Information disclosed in error (email, posted, fax, verbal)	86	0
Lost or stolen hardware	3	0
Lost or stolen paperwork	0	0
Online Disclosure (e.g. website, social media)	0	0
Unauthorised access to IT systems	3	0
Unauthorised access to physical documents	0	0
Corruption or inability to recover information	0	0
Other	3	0
Q3	**112**	**0**
Cyber Attack (e.g. virus, ransomware, phishing email)	1	0
Information disclosed in error (email, posted, fax, verbal)	91	0
Inability to recover hardware	1	0
Lost or stolen hardware	4	0
Lost or stolen paperwork	4	0
Online Disclosure (e.g. website, social media)	1	0
Unauthorised access to IT systems	6	0
Unauthorised access to physical documents	0	0
Corruption or inability to recover information	0	0
Non-secure disposal of paperwork	1	0
Other	3	0
Q4	**134**	**0**
Cyber Attack (e.g. virus, ransomware, phishing email)	0	0
Information disclosed in error (email, posted, fax, verbal)	93	0

Inability to recover information	0	0
Lost or stolen hardware	4	0
Lost or stolen paperwork	0	0
Online Disclosure (e.g. website, social media)	3	0
Unauthorised access to IT systems	2	0
Unauthorised access to physical documents	1	0
Verbal Disclosure	0	0
Corruption or inability to recover information	2	0
Non-secure disposal of paperwork	0	0
Lost away from office	1	0
Other	28	0

C2 – Summary of personal data breaches submitted to the ICO

Ref.	Incident reported	Summary of the personal data breaches investigated by the Information Commissioner's Office	INCIDENT TYPE
W2L6	04/2022	Personal data breach regarding the inappropriate disclosure of confidential concerns affecting two people. ICO considered the appropriate technical and organisational measures in place and the low likelihood the data would be misused. No further action from ICO.	Information disclosed in error
W9W9	04/2022	Personal data breach regarding the meeting minutes being shared with a third party. Reviewing systems so that personal data isn’t automatically carried forward was completed. No further action from ICO.	Information disclosed in error
P6C5	05/2022	Personal data breach regarding the sharing of basic personal identifiers, ie name within a spreadsheet. Process amended to prevent a recurrence. No further action from ICO.	Information disclosed in error

Appendix D: Investigatory Powers Commissioner Office Return

Sheffield City Council		Volume
Covert Human Intelligence Sources (CHIS) & Juvenile Covert Human Intelligence Sources (Juvenile CHIS)	The number of applications made for a CHIS authorisation?	0
	Of these, the number of applications made for a Juvenile CHIS authorisation?	0
	The number of CHIS authorisations successfully granted?	0
	Of these, the number of Juvenile CHIS authorisations successfully granted?	0
	The number of urgent applications made for a CHIS warrant?	0
	Of these, the number of urgent applications made for a Juvenile CHIS authorisation?	0
	The number of CHIS authorisations granted in an urgent case?	0
	Of these, the number of Juvenile CHIS authorisations granted in an urgent case?	0
	The number of CHIS authorisations that were renewed?	0
	The number of CHIS authorisations that were cancelled?	0
	The number of CHIS authorisations extant at the end of the year?	0
	The age of the Juvenile CHIS at the time of the authorisation's issue? (to be completed in rows below)	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
	Juvenile CHIS age at application	0
	Quantity	0
Directed Surveillance (RIPA & RIPSA)	The total number of applications made for a Directed Surveillance authorisation (including renewals)?	9
	The total number of Directed Surveillance authorisations successfully granted (including renewals)?	9
	The number of urgent applications made for a Directed Surveillance authorisation?	0

This page is intentionally left blank

Audit and Standards Committee Report

Report of: **Chief Operating Officer**

Date: **19/10/2023**

Subject: **Information Commissioner's Office (ICO) FOI Audit Report**

Author of Report: **Sarah Green**
Senior Information Management Officer and Data Protection Officer

Summary: **In May 2023, the ICO carried out a consensual audit of the Freedom of Information (FOI) practices at Sheffield City Council. This took place over two days in May 2023. Sheffield City Council received a set of recommendations from the ICO following the audit.**

Recommendations: To note the audit update

Background Papers: None

Category of Report: OPEN

Statutory and Council Policy Checklist

Financial Implications
NO
Legal Implications
YES
Equality of Opportunity Implications
NO
Tackling Health Inequalities Implications
NO
Human rights Implications
NO
Environmental and Sustainability implications
NO
Economic impact
NO
Community safety implications
NO
Human resources implications
NO
Property implications
NO
Area(s) affected
None
Relevant Cabinet Portfolio Member
Councillor Cate McDonald
Is the item a matter which is reserved for approval by the City Council?
NO
Press release
NO

REPORT TITLE: Information Commissioner’s Office (ICO) FOI Audit Report

1.0 INTRODUCTION

1.1 This report has been written to provide an overview of the Information Commissioner’s Office (ICO) consensual audit of the FOI practices at Sheffield City Council and to provide assurance around the recommendations given by the ICO, to ensure that we meet our legal obligations.

2.0 BACKGROUND

2.1 Following the publication of the Lowcock report, SCC agreed to a request from the Information Commissioner’s Office (ICO) for a consensual FOI audit to be undertaken. This took place over 2 days in May 2023.

2.2 An ICO FOI audit provides an assessment of the organisation of its FOI practices. It is a useful tool in supporting the organisation in both understanding and meeting its obligations under the Freedom of Information Act 2000 (FOIA).

2.3 An ICO audit looks at the controls the organisation has in place, its policies and procedures and provides recommendations.

2.4 An ICO audit is an opportunity for the organisation to get an independent view of its practices, and to provide focussed feedback. The ICO sees auditing as a constructive process with benefits for public authorities.

2.5 An ICO audit is beneficial to the organisation, as it provides the organisation with specialised expertise and knowledge and a robust set of actions to support its best practice.

3.0 THE AUDIT

3.1 The ICO contacted the organisation in April 2023 to ask if it was amenable to an audit focusing on its FOI practices.

3.2 The organisation agreed to the audit and in May 2023 the ICO spent two days conducting the FOI audit. Before this, there was some preparation work, in order to provide the auditor with as much information as possible ahead of their visit. This included policies and procedures.

3.3 Following completion of the audit, around 30 days later, the ICO provided a comprehensive report, along with an executive summary.

3.4 In July 2023 the ICO published the executive summary on its website.

4.0 THE RECOMMENDATIONS AND TIMELINES

4.1 The audit report focuses on risk and observations made by the auditor. The report gives its recommendations by priority (Appendix A).

4.2 The assurance ratings range from high assurance to very limited assurance.

5.0 OUR ASSURANCE RATING

5.1 The ICO gave an assurance rating of 'Reasonable' to the organisation.

5.2 The overall opinion is that there is a reasonable level of assurance that processes and procedures are in place to deliver FOI compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the FOIA

5.3 There were 13 recommendations that the ICO made. These were broken down into priority recommendations. (See Appendix B).

5.4 The assurance rating was also broken down from high to very limited assurance. (See Appendix C).

6.0 AREAS FOR IMPROVEMENT

6.1 The ICO recognises that the organisation provides training to staff, however a recommendation is that training on FOI and information management is developed further so that all staff can easily locate and retrieve information to be included in responses.

6.2 The ICO has also recommended that those staff who handle FOI requests as part of their role, have further developed training to support their understanding of the exemptions and legislation.

6.3 The organisation should improve how it anticipates where a proposal or event may place demand on the organisation, and have procedures in place to respond proactively, to avoid future backlogs.

6.4 The organisation should proactively publish more information to help manage demand.

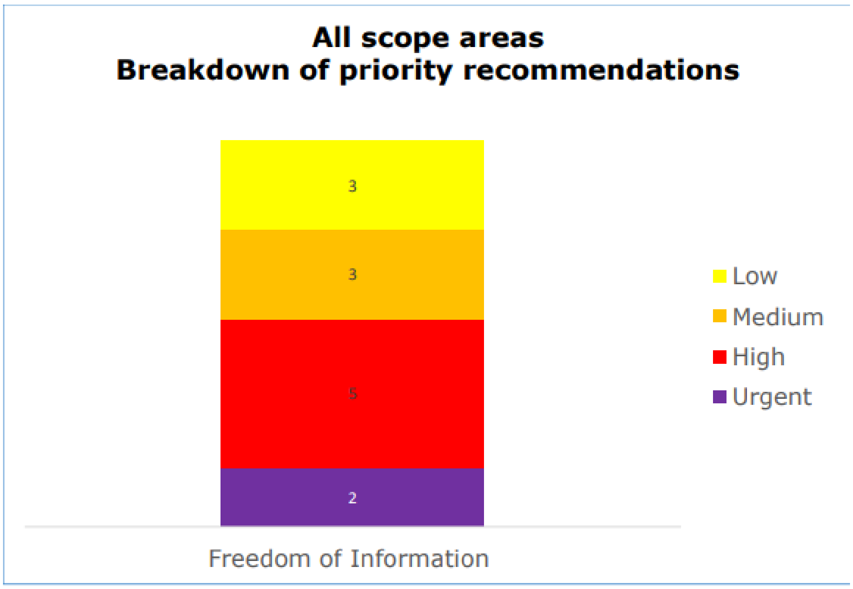
7.0	**BEST PRACTICE**
7.1	The ICO noted that the staff interviewed reflected the importance of FOI within its organisational values, 'openness and honesty are important to us'.
8.0	**ICO RECOMMENDATIONS AND PRIORITY**
8.1	SCC should carry out a review of service contacts to determine whether requests issued to service areas are being handled by the most appropriate personnel – Low Priority
8.2	SCC should review the staffing level of the IM Team - Urgent Priority
8.3	a) SCC must publish a schedule of fees if it is to continue charging fees for any information made available under its publication scheme, whether under the FOI or EIR. b) SCC should address any backlogs of information that it has committed to publishing proactively – High Priority
8.4	SCC should ensure that service areas have documented processes in place so that requests are handled consistently – Medium Priority
8.5	SCC should update its FOI procedures to account for hybrid FOI and data subject requests – Low Priority
8.6	SCC should continue with its work to identify a suitable casework management system and implement this as soon as possible – High Priority
8.7	SCC should introduce further, documented quality assurance measures to be applied to final responses issued by the IM Team – Low Priority
8.8	a) SCC should monitor service areas' compliance to the 10-day internal deadline. b) SCC should ensure that FOI is considered from the outset where new policy initiatives are to be introduced or where significant events can be anticipated. – Urgent Priority
8.9	SCC should revise its procedure for handling internal reviews so that there is greater assurance that outcomes are impartial. SCC should ensure that internal reviews are formally logged. – High Priority

8.10	SCC should revise the resources available to its IM Team covering the application of exemptions – High Priority
8.11	SCC should introduce a process for submissions to the Monitoring Officer for the purpose of applying Section 36 – Medium Priority
8.12	SCC should introduce separate, mandatory training for all staff covering FOI and information management. This should be refreshed every two years This should be monitored for completion by all staff – High Priority
8.13	SCC should provide additional training to service contacts to ensure that they are aware of their responsibilities and have the knowledge required to carry out their role effectively – Medium Priority
9.0	**PROGRESS ON RECOMMENDATION ACTIONS**
9.1	The timelines for implementing the recommendations range from autumn 2023 to summer 2024.
9.2	A number of recommendations have already been actioned, this includes the training programme for staff and identifying a case management system
9.3	SCC has commissioned PwC to support the review and to provide independent advice on implementing the recommendations in relation to process improvements and the sustainability of the service.
9.4	There has been an amendment to how the organisation monitors its FOIs by improving the visibility of each stage for tracking and responding.
9.5	There has been a new suite of learning and training resources made available to all staff.
9.6	Hybrid requests have been included in processes.
9.7	The process map for FOI has been significantly enhanced and reviewed and revised to identify areas for improvement and improved productivity.
9.8	A number of case management systems have been identified that will publish information requests automatically, to improve transparency.
9.9	The Council is currently reviewing an in-house solution for the tracking and monitoring of FOIs to support with compliance.

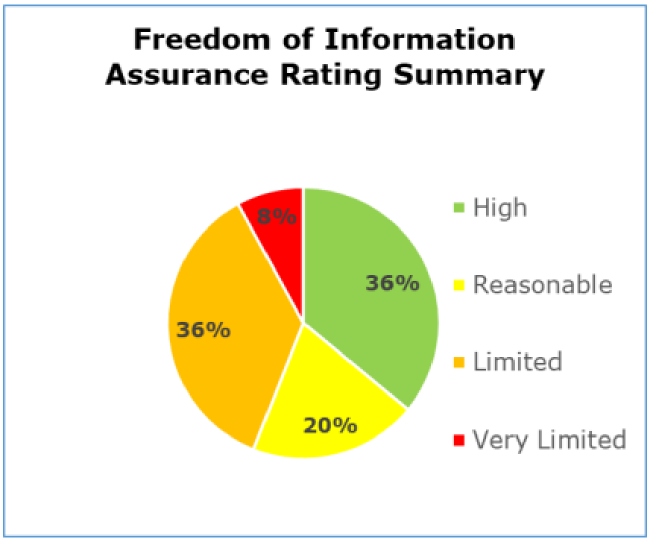
9.10	The Council, together with support from PwC, are reviewing the sustainability of the Service to ensure its size and technological support meets the demands placed on it.

Appendix A: Attached

Appendix B: Breakdown of Priority Areas



Appendix C: Assurance Rating Summary



This page is intentionally left blank

ICO Data Protection Audit - Action Plan

Controller	Sheffield City Council
Report Date	Jun-23

Audit Action Plan										Audit Action Plan Update		
Ref	Control measure	Non-conformity	Recommendation	Priority	Accept / Partially Accept / Reject	Agreed Action	Implementation Date	Owner	Update at xx months	Update at xx months	Action Status	Evidence item(s) provided
A.2.	Individual responsibility has been assigned to ensure compliance with FOI/EIR.	Within SCC's central IM Team, clear roles and responsibilities have been assigned in relation to the handling of FOI requests and overall compliance. Staff members within service areas are also designated as 'service contacts', and are responsible for providing responses to requests issued by the IM Team. However, during interviews with staff from various service areas, it became apparent that being able to provide responses often relied on information from members of staff within service areas who are not designated service contacts. This may mean that responsibility for handling requests is not always assigned to the correct personnel. This is likely to lead to delays, which may result in statutory deadlines being	SCC should carry out a review of service contacts to determine whether requests issued to service areas are being handled by the most appropriate personnel.	Low	Accept	FOI Team to audit Service Contacts and update with the support of each Service. Already started.	Sep-23					#REF!B2:N15:N11:N26:N10:H
A.3.	Sufficient resources are assigned to the handling of requests for information to ensure response within the statutory timescales	SCC has adopted a 'centralised' model for handling FOI requests. Incoming requests are triaged by a central IM Team, who allocate these to the service areas within the organisation which are likely to hold relevant information. These service areas then have 10 days to locate and return any relevant information to the IM Team, who are responsible for applying exemptions and redactions (where necessary) before issuing a response. The IM Team has a staffing level of just 2.25 FTE, which is relatively low given the size of SCC and volume of FOI requests it receives. In interview, it was established that temporary staff have been required on one occasion to help address backlogs. The IM Team were	SCC should review the staffing level of the IM Team, with respect to its workload, and consider whether additional resource would help to eliminate existing backlogs and to avoid future backlogs. With more resources, the IM Team could also help to ensure that information is proactively published wherever possible, which would likely reduce the number of requests received by increasing transparency.	Urgent	Accept	Review of Information Management Team Operating Model to improve resourcing of information requests.	Jul-24					
A.4.	The organisation has an ICO approved publication scheme in place.	SCC has adopted the ICO's Model Publication Scheme and publishes information in line with this scheme via its own website, and via a collaborative website called Data Mill North. In interview, it was found that SCC charges fees in some cases for the release of environmental information made available under its publication scheme. However, SCC has not published a schedule of fees alongside its publication scheme, meaning that fees charged for the release of any information under the scheme are in breach of Regulation 8 of the EIR. During interviews, it also became apparent that SCC has fallen behind in its proactive publication of information in some areas. A backlog of previous FOI responses which were intended for publication	**A.4.a.** SCC must publish a schedule of fees if it is to continue charging fees for any information made available under its publication scheme, whether under the FOI or EIR. **A.4.b.** SCC should address any backlogs of information that it has committed to publishing proactively. Information intended for publication should be published within a reasonable timescale.	High	Accept	A.4.a IM to liaise with Legal to publish charging fees A.4.b IM to implement new case management system to automate publishing. SCC to consider staffing resource to publish previous requests	A.4.a - 01/09/2023 A.4.b 01/07/2024 (part of review of operating model)					

A.5.	Policies and procedures are in place which explain the organisation's approach to, and responsibilities for, FOI and EIR regulations	SCC has an FOI and EIR policy, as well as a standard operating procedure. There are also other supporting procedures in place which cover administrative aspects of handling requests. However, these policies and procedures don't cover the handling of requests within service areas, with respect to the process involved in locating and retrieving information. Only one procedure was seen which outlined the handling of requests within a service area, with the document metadata showing that this had only recently been created. Whilst evidence was seen during interviews that service areas had their own request trackers and systems in place, there was no evidence that staff in these areas were following documented processes. A	SCC should ensure that service areas have documented processes in place so that requests are handled consistently. Processes should outline the searches that are likely to be necessary and the personnel that may need to be consulted.	Medium	Accept	FOI Team to work with Services to document their process comprehensively with reference to the nature of their information and information systems.	01/10/23					
A.6.	Policies and procedures for FOI/EIR account for personal information and how it should be dealt with	During interviews various members of staff displayed a good level of awareness of how requests for personal data should be handled, and of the need to redact personal data from FOI responses in most cases. However, SCC's FOI procedures don't provide any guidance on how requests for personal data of both the requester and others ('hybrid requests') should be handled. This creates a risk of inappropriate disclosures of personal data.	SCC should update its FOI procedures to account for hybrid requests so that these are handled correctly and according to the ICO's guidance.	Low	Accept	To revise the FOI SoP for this purpose.	31/07/23					
A.7.	The organisation maintains a documented record of their receipt and handling of requests	SCC maintains records of its receipt and handling of requests across three systems; an Outlook inbox, a platform called '4me' which is used to track the progress of request handling, and a Sharepoint area which is used to store original and redacted versions of documents where necessary. Whilst SCC is able to maintain adequate records in this way, it became clear during interviews that this is not the most effective or efficient way to do so. Interviewees explained that the '4me' platform used to track requests was more suited for use by IT service desks, and that it had been difficult to extract to necessary data from this platform to effectively monitor the handling of FOI requests. Interviewees	SCC should continue with its work to identify a suitable casework management system and implement this as soon as possible.	High	Accept	3 case management systems shortlisted following research. Final review underway and procurement exercise being prepared. Budget being sourced.	01/07/2024, linked to Op.Model					
A.8.	There are mechanisms to monitor the quality of responses to requests	SCC's Freedom of Information Standard Operating Procedure sets out criteria by which responses from service areas are assessed. Final responses prepared by an Information Access Officer (IAO) are also reviewed by an Information Management Officer (IMO) to provide assurance on the application of exemptions and redactions. However, there are no formal mechanisms or documented processes in place to monitor and ensure the quality of final responses issued by the IM Team. Without more formal quality assurance measures, responses to requests may be inconsistent and SCC may receive a higher number of complaints.	SCC should introduce further, documented quality assurance measures to be applied to final responses issued by the IM Team.	Low	Accept	To update the SoP quality assurance measures to be applied by final responses. Review of Information Management Team Operating Model to improve resourcing of information requests to ensure monitoring of quality assurance.	01/12/23					

A.9.	The organisation is complying with statutory timescales for FOI/EIR regulations.	SCC is making significant efforts to improve compliance with statutory timescales for FOI and EIR regulations. Urgent priority has been given to a delivery plan to improve performance in this area and organisation-wide efforts have been made in support of this plan. However, compliance with statutory timescales is still unsatisfactory on the whole, according to the ICO's criteria. The ICO audit has identified two factors which are likely to be affecting performance. Firstly, SCC doesn't appear to have sufficient insight as to where delays occur and backlogs accumulate. Service areas have a 10 day internal deadline to provide their response to an FOI request to the IM Team. However, adherence to this	**A.9.a.** SCC should monitor service areas' compliance to the 10 day internal deadline. Compliance should be reported to the appropriate oversight board or committee. Where a service area is routinely missing this deadline, action should be taken to assist this service area in improving its compliance. **A.9.b.** SCC should ensure that FOI is considered from the outset where new policy initiatives are to be introduced or where significant events can be anticipated. In these cases, SCC should put a plan in place to proactively publish relevant information.	Urgent	Accept	Review of Information Management Team Operating Model to improve resourcing of information requests.	01/07/2024 Review of Operating Model completed by Jul 24					
A.10.	Internal review procedures comply with the relevant Codes of Practice and ensure that timely responses are provided to complaints.	SCC has a procedure in place for internal reviews, which sets out that these should be carried out by a member of the IM Team who was not involved in processing the initial request. However, the procedure also states that the majority of internal reviews will be handled by an IMO. There is only one IMO within the IM Team who works on FOI, and during interviews it became clear that they typically provide input to the handling of requests. Therefore, it's unlikely internal reviews are handled by a member of the IM Team who was not involved in processing the initial request. This means that the outcomes of internal reviews are less likely to be truly impartial, which may result in a higher number of complaints to the ICO. SCC	**A.10.a**. SCC should revise its procedure for handling internal reviews so that there is greater assurance that outcomes are impartial. The ICO recognises that limited resource is a factor which influences the current approach. The additional resource recommended in A.3. would also help to enhance the internal review process. **A.10.b.** SCC should ensure that internal reviews are formally logged within a log of complaints or similar, so that their progress and outcomes can be monitored.	High	Accept	A10.a - This will be linked to the new Operating Model, where we are reviewing resource. A10.b - Log of complaints is being updated.	Jul 24 as linked to Operating Model					
A.11.	Exemptions/Exceptions should be applied on a case-by-case basis, by appropriately trained staff, with no evidence of the use of blanket exemptions/exceptions.	Whilst SCC's 'centralised' approach to handling FOI requests means that staff from across the organisation are involved in this process, only staff within the IM Team may apply exemptions. The staff within this team have received training and have significant experience in this area. However, there is concern that some of the resources available to this team may not be explanatory and expansive enough to ensure that exemptions are always applied with consideration of all the key criteria. This creates a risk that the exemption may be applied without proper consideration, and that information may be wrongly withheld.	SCC should revise the resources available to its IM Team covering the application of exemptions. Any and all resources of this kind should set out all of the key criteria to fulfil before applying a particular exemption.	High	Accept	Will update the documentation and publish to Sharepoint.	31/07/23					
A.12.	There is evidence of an oversight or approval process for the use of exemptions/exceptions.	In general, exemptions are applied by an IAO within the IM Team, with the daily oversight and assistance of an IMO. In complex cases, approval is also sought from the IM Team manager. In order to apply the exemption under Section 36 (Prejudice to the effective conduct of public affairs), the input of SCC's Monitoring Officer is sought. As SCC's 'qualified person' under Section 36, the Monitoring Officer needs to provide their reasonable opinion that the exemption is engaged. A submission is sent to the Monitoring Officer by the IM Team when they require this opinion. However, evidence seen by the ICO raises concerns that this submission may not always provide the detail required for the Monitoring Officer to	SCC should introduce a process for submissions to the Monitoring Officer for the purpose of applying Section 36. This process should ensure that submissions always include all of the information to which the exemption would be applied, a thorough explanation of what would be prejudiced or inhibited and how, and any other information relevant to the context and circumstances of the request.	Medium	Accept	The form will be reviewed and amended to ensure it is more explanatory. A process will be written to sit alongside the form to support the staff submitting the form to the Monitoring Officer	01/09/23					

A.13.	There is an induction training programme, with input from Information Governance or equivalent, which includes general training on how FOI/EIR applies to the organisation, what they currently do to comply, and how to recognise an FOI/EIR request.	SCC has mandatory induction training for all staff on data protection and handling information, which in part also covers FOI. This training must be completed by all staff and refreshed annually, or access to systems is revoked. Unfortunately, the content of this training was not provided as part of the evidence submitted by SCC, but it is clear from other evidence submitted that this training does not provide extensive guidance on FOI. Moreover, the training would seem to focus on handling information from a data security perspective, rather than an information management perspective. Training staff to manage information effectively is likely to assist in improving overall FOI compliance, as service areas should be able	**A.13.a.** SCC should introduce separate, mandatory training for all staff covering FOI and information management. The training should provide staff with a basic understanding of FOI and how they need to store and handle information so that requests can be fulfilled. **A.13.b.** The FOI and information management training should be refreshed at least every two years. **A.13.c.** Completion of the FOI and information management training should be monitored to ensure that this is completed by all staff.	High	Accept	A13.a - All staff must engage with the yearly mandatory training in data security and protection. Up to and including 2022, it did include FOI. In 2023 SCC used an off the shelf product that did not include FOI. We will include it in our bespoke course from 2024. The bespoke course will be greater in depth, to ensure staff are reminded on the importance of being able to store, locate and retrieve information effectively. A.13.b. - We will review every 2 years A.13.c - Staff training is monitored by the Learning and Development Team,	01/10/23					
A.14.	There is specific training for staff with responsibility for handling requests for information, on FOI, EIR and Codes of Practice.	Members of SCC's IM Team have undertaken specific training to provide them with knowledge and expertise required to carry out their role, in particular around applying exemptions. However, service contacts also have specific responsibility for handling requests for information, and do not receive any additional training to support this. In particular, service contacts are responsible for identifying where the cost of complying with a request would exceed the appropriate limit (Section 12). Without training or guidance on this, there is a risk that requests could be refused under Section 12 inappropriately.	SCC should provide additional training to service contacts to ensure that they are aware of their responsibilities and have the knowledge required to carry out their role effectively. The training should cover the application of Section 12. The ICO has produced guidance on this which may help inform the content of this training.	Medium	Accept	Useful feedback that we are keen to implement.	01/10/23					

Agenda Item 9

Audit and Standards Committee Report

Report of: General Counsel

Date: 19 October 2023

Subject: Work Programme

Author of Report: Jay Bell, Democratic Services

Summary:

The report provides details of an outline work programme for the Committee.

Recommendations:

That the Committee:-

(a) considers the Work Programme and identifies any further items for inclusion; and

(b) approves the work programme.

.

Background Papers: None

Category of Report: OPEN

Statutory and Council Policy Checklist

Financial Implications
NO Cleared by:
Legal Implications
NO Cleared by:
Equality of Opportunity Implications
NO Cleared by:
Tackling Health Inequalities Implications
NO
Human rights Implications
NO:
Environmental and Sustainability implications
NO
Economic impact
NO
Community safety implications
NO
Human resources implications
NO
Property implications
NO
Area(s) affected
NONE
Is the item a matter which is reserved for approval by the City Council?
NO
Press release
NO

REPORT OF THE GENERAL COUNSEL

AUDIT AND STANDARDS COMMITTEE
19 October

WORK PROGRAMME

1. **Purpose of Report**

1.1 To consider an outline work programme for the Committee.

2. **Work Programme**

2.1 It is intended that there will be at least five meetings of the Committee during the year with three additional meetings arranged if required. The work programme includes some items which are dealt with at certain times of the year to meet statutory deadlines, such as the Annual Governance Report and Statement of Accounts, and other items requested by the Committee. In addition, it also includes standards related matters, including an annual review of the Members Code of Conduct and Complaints Procedure and an Annual Report on the complaints received.

2.2 An outline programme is attached and Members are asked to identify any further items for inclusion.

3. **Recommendation**

3.1 That the Committee:-

(a) considers the Work Programme and identifies any further items for inclusion; and

(b) approves the work programme.

David Hollis
General Counsel

This page is intentionally left blank

4.0 Referrals from other Committees

4.1 Any referrals sent to this Committee by Council, including any public questions, petitions and motions, or other committees since the last meeting are listed here, with commentary and a proposed course of action, as appropriate:

Issue	
Referred from	
Details	
Commentary/ Action Proposed	

Part 5: Proposed additions and amendments to the work programme since the last meeting:

Item	Proposed Date	Note
Community Schools Update	From October 2023 to February 2024	Work is yet to be completed
Fargate Containers	From October 2023 to November 2023	Agreed by members at pre-agenda meeting on 10/10/2023

Part 6: Audit & Standards Committee Work Programme for municipal year 2023/24:

Date	**Item**	**Author**
June 2023	Audit Training	External Facilitator (TBC)
22 June 2023	Internal Audit Tactical Plan 23/24	Linda Hunter (Senior Finance Manager)
	Compliance to International Auditing Standards	Tony Kirkham (Interim Director of Finance and Commercial Services)
	Audit Recommendation Tracker Progress Report	Linda Hunter (Senior Finance Manager)
	Update on Governance Issues outlined in the Annual Governance Statement	David Hollis (Interim General Counsel/Monitoring Officer)

	Summary of Statement of Accounts	Tony Kirkham (Interim Director of Finance and Commercial Services)
	Work Programme	David Hollis (Interim General Counsel/Monitoring Officer)
	Strategic Risk Update	Helen Molteno (Corporate Risk Manager)
27 July 2023	Internal Audit Annual Fraud Report	Stephen Bower (Finance and Risk Manager)
	Role of the Audit Committee and Training	Claire Sharratt (Senior Finance Manager)
	Update on Improvement Plan and Annual Complaints Report 22/23	Corleen Bygraves-Paul (Service Delivery Manager, Customer Services)
	Work Programme	David Hollis (Interim General Counsel/Monitoring Officer)
21 September 2023	External Audit Plan 2021/22	External Auditor (EY)
	Annual Internal Audit Report	Linda Hunter (Senior Finance Manager)
	Statement of Accounts 2021/22 (Audited)	Philip Gregory (Director of Finance and Commercial Services)
	Interim Standards Complaints Report (Half Yearly)	David Hollis (Interim General Counsel/Monitoring Officer)
	Work Programme	David Hollis (Interim General Counsel/Monitoring Officer)
19 October 2023	Workshop to Review Members' Code of Conduct and Complaints Procedure	

19 October 2023	Information Management Annual Report & ICO Audit	Sarah Green (Senior Information Management Officer)
	Work Programme	David Hollis (General Counsel/Monitoring Officer)
23 November 2023	Report of those Charged with Governance (ISA 260)	External Auditor (EY)
	Formal Response to Audit (ISA 260) Recommendations	Philip Gregory (Director of Finance and Commercial Services)
	Update on Ombudsman Report for 22/23	Corleen Bygraves-Paul (Service Delivery Manager, Customer Services)
	Annual Governance Statement	David Hollis (General Counsel/Monitoring Officer)
	Review of Members' Code of Conduct and Complaints Procedure	David Hollis (General Counsel/Monitoring Officer)
	Fargate Containers	David Hollis (General Counsel/Monitoring Officer)
	Work Programme	David Hollis (General Counsel/Monitoring Officer)
11 January 2024	Statement of Accounts 2022/23 (Audited)	Philip Gregory (Director of Finance and Commercial Services)
	Whistleblowing Policy Review	Elyse Senior-Wadsworth (Head of Human Resources)
	Annual Standards Report	David Hollis (General Counsel/Monitoring Officer)
	Audit Recommendation Tracker Progress Report	Linda Hunter (Senior Finance Manager)
	Strategic Risk Reporting	Helen Molteno (Corporate Risk Manager)
	Work Programme	David Hollis (General Counsel/Monitoring Officer)

1 February 2024	Complaints performance and complaints Service improvement plan	Corleen Bygraves-Paul (Service Delivery Manager, Customer Services)
	Community Schools Update	Andrew Jones (Director of Education and Skills)
	Work Programme	David Hollis (General Counsel/Monitoring Officer)
21 March 2024	Work Programme	David Hollis (General Counsel/Monitoring Officer)
25 April 2024	Internal Audit Plan 2024/25	Linda Hunter (Senior Finance Manager)
	Compliance to International Auditing Standards	Philip Gregory (Director of Finance and Commercial Services)
	Work Programme	David Hollis (General Counsel/Monitoring Officer)
July / August 2024	Audit Training	External Facilitator (TBC)
June 2024	Audit Recommendation Tracker Progress Report	Linda Hunter (Senior Finance Manager)
	Strategic Risk Update	Helen Molteno (Corporate Risk Manager)
	Work Programme	David Hollis (General Counsel/Monitoring Officer)

IMPORTANT INFORMATION FOR REPORT WRITERS

The Audit and Standards Committee provides an independent and high-level focus on the audit, assurance and reporting arrangements that underpin good governance and financial standards.

The purpose of the Committee is to provide independent assurance to the Council of the adequacy of the risk management framework and the internal control environment. It provides independent review of Sheffield City Council's governance, risk management and control frameworks and oversees the financial reporting and annual governance processes. It oversees internal audit and external audit, helping to ensure efficient and effective assurance arrangements are in place.

The Committee also cover Standards and is primarily responsible for promoting and maintaining high standards of conduct by councillors, independent members, and co-opted members. It is responsible for advising and arranging relevant training for members relating to the requirements of the code of conduct for councillors. The Committee also monitor the Council's complaints process and the Council's response to complaints to the Ombudsman.

The Committee is not an operational committee, so is not focussed on the day to day running of your service. However, its focus is on risk management and governance, so it will want to understand how you manage your key risks, and how you are responding to new challenges and developments. In particular the Committee will be interested in the progress on implementing agreed recommendations from inspection and audit reports, and will want to review your services' outputs and actions in response. You can expect some challenge if deadlines for implementing agreed actions have been missed. Please ensure breakdowns of information are included in your report, as the Committee is interested in the key facts and figures behind areas.

Most Audit and Standards papers are public documents, so use everyday language, and use plain English, don't use acronyms, or jargon and explain any technical terms. Assume the reader knows little about your subject.

Think about how the paper will be interpreted by those who read it including the media.

Use standard format - don't subvert it.

***Ensure* –** You convey the key message in the first paragraph not the last.

The report should include –

- ***Summary***
- ***Recommendation (s)***
- ***Introduction***
- ***Background***
- ***Main body of the report (in. legal, financial and all other relevant implications)***

(report templates are available from Democratic Services)

This page is intentionally left blank