Audit and Standards Committee Report

Title of Report: Information Governance Annual Report

Date of Decision: N/A

Report To: Audit and Standards Committee

Report Of: David Hollis, General Counsel

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

Executive 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.

Does the report contain confidential or exempt information? No

Recommendations:

The Audit and Standards Committee is recommended to:

1. Note the annual information governance update.

Financial Implications: No

Legal Implications: No

Equality and Inclusion Implications: No

Climate Change Implications: No

Background Papers: None

Appendices:

Appendix A-1: FOI and EIR Requests Response Performance 2023/24

Appendix A-2: Yearly FOI and EIR Requests Response Performance

Appendix B-1: Subject Access Request Performance 2023/24

Appendix B-2: Yearly Subject Access Request Performance

Appendix C-1: Reported Information Security Incidents and Personal Data Breaches - Quarterly figures 2023/24

Appendix C-2: Summary of personal data breaches submitted to the ICO

Appendix D: Investigatory Powers Commissioner's Office Return

Background to the issue

N/A

1. Proposal

N/A

2. Equality and Inclusion Implications

There are no equality and/or inclusion implications arising from the report.

3. Financial and Commercial Implications

There are no financial and/or commercial implications arising from the report.

4. Legal Implications

There are no legal implications arising from the report. However, failure to comply with the UK GDPR, Data Protection Act 2018, Freedom of Information Act 2000, Environmental Information Regulation 2004 and Regulation of Investigatory Powers Act 2000 could have legal implications for the Council.

5. Climate and Environmental Implications

There are no climate and/or environmental implications arising from the report.

REPORT TITLE: Information Governance Annual Report for 2023/24

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.
1.2	It is important to note that this is a retrospective report, covering the financial year 2023/24.
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, Directorate 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	2023/24 was the sixth financial year in which the GDPR (now the UK GDPR) and the DPA have been in force.
3.2	2017/2018 and 2018/2019 were spent preparing for GDPR, 2019/20 adapting to the new law and 2020/21 and 2021/22 were significantly impacted by the coronavirus pandemic.
3.3	In September 2021, the Conservative Government began to prepare for a shake-up of UK data protection law with a consultation 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 Bill was abandoned when the General Election was called. The new Labour Government have announced a Digital Information and Smart Data Bill (DISD) which will target reforms to some data laws.
3.4	The Council has continued to work to ensure compliance with the law.
3.5	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 2024/25 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 2023/24, the Council received 1057 Subject Access Requests. 517 requests were either withdrawn or abandoned by the requester and 540 were actioned. 398 of these were answered in time (see Appendix B). The overall SAR performance figure for 2023/24 is 73.7%.
4.5	Unlike FOIA and EIR, the DPA and UK GDPR do not give the requester the specific right to appeal about the way their request has been handled. However, the ICO expects requesters to have complained to the organisation and the organisation to have taken steps to resolve the issues before they will look at a complaint. The Council received 14 such SAR Complaints in 2023/24.
4.6	In 2023/24, the Council responded to sixteen SAR Complaints. Three of these were originally received in 2021/22, seven in 2022/23 and six in 2023/24. Three SAR Complaints were withdrawn in 2023/24, when Requesters failed to respond to our requests for clarification.
4.7	Eight SAR Complaints from 2023/24 remained outstanding on 31 March 2024.
4.8	The ICO has corresponded with the Council about seven complaints regarding Subject Access Requests in 2023/24. The majority of these cases concerned situations where requesters had complained to the ICO because they had not been provided with the information they had requested within the statutory timeframe.
4.9	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 FOIA and 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 2023/24, the Council received 1894 requests and answered 85.2% in time (Appendix A). This is an increase of 16% (306 requests) on the number of information requests received in 2022/23. The response rate is an improvement on the 82.1% achieved in 2022/23 but fails to meet the Information Governance Board's target of 95% of requests answered in time. The ICO considers an acceptable compliance rate to be 90%.
5.4	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 received 56 Internal Reviews in 2023/24.
5.5	The Council completed 73 Internal Reviews in 2023/24. 44 of these were from 2023/24, and 29 were from previous years.
5.6	12 Internal Reviews from 2023/24 remained outstanding on 31 March 2024, as well as another six from previous years.
5.7	In addition to the above, the ICO has corresponded with the Council on 18 occasions concerning FOI/EIR requests in 2023/24. Of these cases, eleven were because we were late with a response to the requester, which we subsequently provided. In the other five cases, the ICO upheld two complaints by a requester, directing the council to disclose information. In the other three cases, the ICO did not uphold requesters' complaints, and did not require the council to take any further steps. Two cases from 2023/24 remain open, and we are awaiting further instruction from the ICO.
6.0	**OPEN DATA**
6.1	Under FOIA, the Protection of Freedoms Act 2012, and the Local Government 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	In 2023/24, 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 11 datasets have been published on Data Mill North. See: Search Datasets | Data Mill North
6.3	The Council also publishes 61 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)
6.4	Further work is ongoing to encourage services within the organisation to recognise the benefits of open data to help demonstrate the Council's commitments to openness, transparency, and public accountability.
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 ICO of personal data breaches that represent a high and ongoing risk to the affected data subjects.
7.2	In 2023/24, 478 incidents were logged through the Council's information security incident process; 354 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, five were considered to meet the risk threshold and were reported to the ICO (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 Directorates. 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 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 (IPCO), which confirms the number of applications that have been considered and submitted to a Magistrate (see appendix D).
8.3	In the calendar year 2023, the Council made two applications for Directed Surveillance (including renewals). These were for the statutory purpose of preventing or detecting crime or of preventing disorder.
8.4	The IPCO 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 demonstrated a good level of compliance that removed, for the present, the requirement for a physical inspection. The IPCO have changed their approach and no longer routinely undertake an inspection. Instead, they will request a written report on compliance. In July 2023, IPCO carried out its usual three-yearly inspection. IPCO responded in writing in November 2023 to provide assurance that ongoing compliance with RIPA and the Investigatory Powers Act 2016 is being maintained. The next inspection is due in 2026.
9.0	**INFORMATION GOVERNANCE RISK AND ISSUES**
9.1	In 2023/24, 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 concerns 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. Increasingly, this includes

	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 Russia'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 it is has full control. A large proportion of Officers are now working at home or in non-council buildings.
10.5	The Council has continually invested heavily in Microsoft technology which support these new ways of working and provide strong security controls. Over this period, Microsoft have continued to develop security tools which we integrate into our security stack, further strengthening the council's position.
10.6	Additional security improvements over this period include the move to a cloud proxy, which protects the user while browsing the internet from malicious content for both on-premise users and remote workers.
10.7	The Council continues to move 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 through processes such as immutability, versioning, and geo-redundancy.
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 ISO 27001 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. This is further supplemented

	with a 24/7 security operations centre to enable continuous monitoring, alerting, and remediating.
10.10	The security threat landscape and associated guidance and controls is forever changing and needs to be constantly monitored and kept under review. A collaborative Cyber Taskforce, represented by colleagues in ICT, Information Management and Information Security has been established to capture, monitor and compare global active cyber-attacks, trends, and campaigns.
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 ICO 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	Data Protection and Information security training is mandatory. 92.2% of our desk-based staff and 47.9% of deskless staff had completed the training. 95.1% of Social Care staff completed the training in time for the 2023/24 NHS Toolkit submission in June 2024.

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

Appendix A-1: FOI and EIR Requests Response Performance 2023/24

	Requests Received	Responses Issued			% Responses Issued within 20 days	% Responses Issued which were overdue
		Within 20 days	Overdue	Total		
Quarter 1	471	334	81	415	**80.5%**	**19.5%**
Quarter 2	470	323	75	398	**81.2%**	**18.8%**
Quarter 3	419	310	47	357	**86.8%**	**13.2%**
Quarter 4	534	376	31	407	**92.4%**	**7.6%**
Full Year	**1894**	**1343**	**234**	**1577**	**85.2%**	**14.8%**

Appendix A-2: Yearly FOI and EIR Requests Response Performance

Financial Year	Number of FOIs	**Compliance %**
2019/20	1942	**93.2**
2020/21	1547	**64.1**
2021/22	1698	**76.2**
2022/23	1586	**82.1**
2023/24	1894	**85.2**

Appendix B-1: Subject Access Request Performance 2023/24

2023/24	Actioned	Answered in time	Answered Late	Compliance %
Quarter 1	70	56	14	**80.0**
Quarter 2	121	84	37	**69.4**
Quarter 3	147	116	31	**78.9**
Quarter 4	202	142	60	**70.3**
Full Year	**540**	**398**	**142**	**73.7**

Appendix B-2: Yearly Subject Access Request Performance

	Received	Actioned*	Answered in time	Answered Late	Compliance %
2017/18	*Not recorded*	192	94	98	**49.0**
2018/19	*Not recorded*	297	219	78	**73.7**
2019/20	*Not recorded*	343	295	48	**86.0**
2020/21	*Not recorded*	303	170	133	**56.1**
2021/22	446	366	228	138	**62.3**
2022/23	809	515	338	177	**65.6**
2023/24	1057	540	398	142	**73.7**

* Not all SARs ‘Received’ are ‘Actioned’. Some SARs are withdrawn by the requester, as the information is no longer needed. Some SARs are abandoned, as the requester does not provide their identification or other necessary information within a reasonable timeframe.

Appendix C-1: Reported Information Security Incidents and Personal Data Breaches - Quarterly Figures 2023/24

	No. of Incidents	ICO Notified
2022 -23		
Q1	**156**	**2**
Corruption or inability to recover information	1	0
Information disclosed in error (email, posted, fax, verbal)	95	2
Lost or stolen paperwork	6	0
Lost or stolen hardware	6	0
Online Disclosure (e.g. website, social media)	0	0
Unauthorised access to IT systems	4	0
Unauthorised access to physical documents	12	0
Cyber Attack	1	0
Non-secure disposal of paperwork	0	0
Other	31	0
Q2	**94**	**2**
Cyber Attack (e.g. virus, ransomware, phishing email)	1	0
Information disclosed in error (email, posted, fax, verbal)	84	1
Lost or stolen hardware	4	0
Lost or stolen paperwork	0	0
Online Disclosure (e.g. website, social media)	0	0
Unauthorised access to IT systems	3	1
Unauthorised access to physical documents	0	0
Corruption or inability to recover information	1	0
Non-secure disposal of paperwork	1	0
Other	0	0
Q3	**94**	**1**
Cyber Attack (inc. spam) (e.g. virus, ransomware, phishing email)	6	0
Information disclosed in error (email, posted, fax, verbal)	60	0
Inability to recover information	2	0
Inability to recover hardware	0	0
Lost or stolen hardware	8	0
Lost or stolen paperwork	5	0
Online Disclosure (e.g. website, social media)	1	1
Unauthorised access to IT systems	7	0
Unauthorised access to physical documents	0	0
Corruption or inability to recover information	4	0
Non-secure disposal of paperwork	0	0
Other	1	0
Q4	**134**	**0**
Cyber Attack (e.g. virus, ransomware, phishing email)	2	0
Information disclosed in error (email, posted, fax, verbal)	115	0
Inability to recover information	0	0
Lost or stolen hardware	3	0

Lost or stolen paperwork	8	0
Online Disclosure (e.g. website, social media)	1	0
Unauthorised access to IT systems	4	0
Unauthorised access to physical documents	1	0
Verbal Disclosure	0	0
Corruption or inability to recover information	0	0
Non-secure disposal of paperwork	0	0
Lost away from office	0	0
Other	0	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
IC-231745-C6F9	Q1	Section 7 Report (a welfare report prepared by social care professionals) was submitted to the Family Court. It contained an incorrect statement. No further action from ICO.	Information disclosed in error
IC-241228-C5T8	Q1	Special category personal data disclosed in error, as part of a restructure. No further action from ICO.	Information disclosed in error
IC-249497-D1G5	Q2	Sheffield City Council implemented a change to its calendars from August 2023. Due to an error in applying the setting rules, all calendar meetings could be opened and any written content or attachment viewed by staff. No further action from ICO.	Information disclosed in error
IC-250406-D3S2	Q2	Unauthorised access to client records. No further action from ICO	Unauthorised access to IT systems
IC-271489-M0W1	Q3	A tenant's new address was disclosed to their abusive ex-partner in a letter. 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)?	1
	The total number of Directed Surveillance authorisations successfully granted (including renewals)?	1
	The number of urgent applications made for a Directed Surveillance authorisation?	0

This page is intentionally left blank