Audit and Standards Committee Report

Report of:	**Interim Director of Legal and Governance and Monitoring Officer**
Date:	**11/01/2023**
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 2021/22

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 2021/22.
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 2021/22 was the fourth 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”. 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 2022/23 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 85% of SARs should be answered on time.

4.4 In 2021/22, the Council handled 446 Subject Access Requests, and answered 228 in time (see Appendix B). The overall SAR performance figure for 2021/22 is 51.1%. It should be remembered that 2021/22 was the second full year of the pandemic with huge disruption to council services.

4.5 The ICO has corresponded with the Council on fifteen separate occasions arising from complaints by data subjects concerning Subject Access Requests in 2021/22. The majority of the cases concerned situations where individuals complained to the ICO that they were not provided with the information to which they were entitled within the statutory timeframe. These complaints were upheld. On two occasions, the ICO disagreed with the exemption applied and requested that the Council disclose the information to the complainant.

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 2021/22, the Council received 1691 requests and answered 75.9% in time (Appendix A). This is an increase on the number of information requests received in 2020/21, by approximately 150 requests. The response rate is an improvement on 64.64% 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 compliance rate for FOIs increased each quarter in 2021/22, with Quarter 4 achieving a compliance rate of 86.15%. The improvement in the compliance rate is in line with the work which has taken place across portfolios to address the backlog and to improve the Council's compliance rates. This also includes the move to an online automated platform that has optimised processes.
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 has handled 44 Internal Reviews from requests that were received in 2021/22. 16 Internal Reviews remain outstanding. Of the 28 Internal Reviews responded to, the majority were resolved: either the Council changed its position and released information or upheld the original decision and was accepted by the requester.
5.6	In addition to the above, the ICO has corresponded with the Council on seventeen separate occasions concerning FOI/EIR requests received in 2021/22. Of these cases, thirteen were in relation to late information requests, which the ICO upheld in favour of the requester. The remaining four complaints were in relation to exemptions applied, and the ICO found in favour of the Council in two of these cases.
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 2021/22, 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 12 datasets have been published on Data Mill North.
6.4	The Council also publishes some open data on the ARC GIS platform (ESRI) which publishes datasets in 6 different categories, including environment, population, planning and transportation.

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 2021/22, 324 incidents were logged through the Council's information security incident process; 108 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, six 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 2021/2022, the Council did not make any applications for Directed Surveillance.
8.4	The Investigatory Powers Commissioner 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. There has been no further contact in 2021/22.
9.0	**INFORMATION GOVERNANCE RISK AND ISSUES**
9.1	In 2021/22, 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	A new mandatory data protection learning module was added to the Sheffield Development Hub in January 2021. 91.30% of Council staff completed the module in 2021/22 with 95.42% of Social Care staff completing the training in time for the 2021/22 NHS Toolkit submission in June 2022.
12.4	Additionally, there has been training of discrete groups such as Foster Carers, student Social Workers and bespoke training for colleagues on Data Protection Impact Assessments, Privacy Notices, and Information Sharing Agreements.

	Some external training was commissioned for staff within the Information Management Team, on data protection. In addition, there has also been specialised training on the Freedom of Information Act for Members. Staff have attended free webinars from solicitors' firms, and national information governance trainers on data protection and Freedom of Information. Project managers attended training on Data Protection Impact Assessments and our People-SARs team attended training on Subject Access Request processing.

Appendix A: FOI and EIR Requests Response Performance 2021/22

		Responses Issued				
	Requests Received	Within 20 days	Overdue	Total	**% of Responses Issued which were issued within 20 days**	**% of Responses Issued which were overdue**
Quarter 1	418	263	122	385	**68.3%**	**31.7%**
Quarter 2	370	272	159	431	**63.1%**	**36.9%**
Quarter 3	432	335	43	378	**88.6%**	**11.4%**
Quarter 4	471	311	50	361	**86.2%**	**13.8%**
Full Year	**1691**	**1181**	**374**	**1555**	**75.9%**	**24.1%**

Appendix B-1: Subject Access Request Performance 21/22

2021/22	Received	Answered in time	Answered Late	**Compliance %**
Qtr 1	91	35	41	**38.5**
Qtr 2	114	54	25	**47.4**
Qtr 3	111	79	41	**71.2**
Qtr 4	130	60	31	**46.2**
Total	446	228	138	**51.1**

Year	Received	Answered in time	Answered Late	**Compliance %**
2017/18	192	94	98	49
2018/19	297	219	78	74
2019/20	343	295	48	86
2020/21	326	170	133	52

Appendix C: Reported Information Security Incidents and Personal Data Breaches

C-1 Quarterly Figures 2021-22

	No. of Incidents	ICO Notified
2021 -22	**324**	
Q1	**108**	**1**
Corruption or inability to recover information	3	0
Information disclosed in error (email, posted, fax, verbal)	82	1
Lost or stolen paperwork	5	0
Lost or stolen hardware	5	0
Online Disclosure (e.g. website, social media)	2	0
Unauthorised access to IT systems	9	0
Unauthorised access to physical documents	1	0
Cyber Attack	1	0
Q2	**74**	**1**
Cyber Attack (e.g. virus, ransomware, phishing email)	3	0
Information disclosed in error (email, posted, fax, verbal)	54	1
Unauthorised access to physical documents	0	0
Lost or stolen paperwork	6	0
Lost or stolen hardware	1	0
Online Disclosure (e.g. website, social media)	1	0
Unauthorised access to IT systems	5	0
Corruption or inability to recover information	4	1
Q3	**70**	**3**
Cyber Attack (e.g. virus, ransomware, phishing email)	1	0
Information disclosed in error (email, posted, fax, verbal)	54	3
Lost or stolen hardware	5	0
Lost or stolen paperwork	3	0
Online Disclosure (e.g. website, social media)	1	0
Unauthorised access to IT systems	1	0
Unauthorised access to physical documents	1	0
Corruption or inability to recover information	4	0
Q4	**72**	**1**
Cyber Attack (e.g. virus, ransomware, phishing email)	1	0
Information disclosed in error (email, posted, fax, verbal)	50	1
Inability to recover information	1	0
Lost or stolen hardware	2	0
Lost or stolen paperwork	1	0
Online Disclosure (e.g. website, social media)	0	0
Unauthorised access to IT systems	4	0
Unauthorised access to physical documents	4	0
Verbal Disclosure	3	0
Corruption or inability to recover information	1	0

Non-secure disposal of paperwork	2	0
Other – use of googlemail, complaint re. disclosure	3	0

C2 – Summary of personal data breaches investigated by the ICO

Ref.	Incident reported	Summary of the personal data breaches investigated by the Information Commissioner's Office	INCIDENT TYPE
SCC 395	11/05/2021	Two people were inadvertently copied into a reply to a member of the public, responding to an informal complaint. The original complaint, whilst ultimately being in the public domain, due its nature, did contain personal data which would have been redacted normally. Staff were reminded of the importance of following the standard practice for sending emails. No further action from the ICO.	Information disclosed in error
R5D1	21/07/2021	Personal details regarding a resident's neighbour were shared inappropriately. The investigation did not find that any personal data had been disclosed inappropriately with other data subjects. No further action from the ICO.	Information disclosed in error
R7T3	22/09/2021	Personal details from a rates account were disclosed to another and a subject access request was not responded to. There was no evidence found to suggest personal information was shared inappropriately. However, the investigation revealed that staff handling the original complaint did not recognise the Subject Access Request within the letter and did not subsequently follow the process by forwarding the request to the Information Management Team. The manager was reminded of the importance of all staff recognising a request for personal information and the staff were required to re-take the GDPR training, to refresh their understanding. No further action from the 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 number of applications made for a Directed Surveillance authorisation?	0
	The number of Directed Surveillance authorisations successfully granted?	0
	The number of urgent applications made for a Directed Surveillance authorisation?	0
	The number of Directed Surveillance authorisation granted in an urgent case?	0
	The number of Directed Surveillance authorisations that were cancelled?	0
	The number of Directed Surveillance authorisations extant at the end of the year?	0

This page is intentionally left blank