Audit and Standards Committee Report

Report of:	**Director of Business Change and Information Solutions**
Date:	**16/12/2021**
Subject:	**Information Governance Annual Report**
Author of Report:	**Mike Weston** **Assistant Director of ICT Service Delivery** **Senior Information Risk Owner**

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 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 2020/21

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 we meet our legal requirements. It is important to note that this is a retrospective report, covering the year 2020/21. This report includes the impact of COVID-19 on performance.
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, information 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, the 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 the Information Governance activity across the Council 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	2020/21 was the third 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	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 2021/22 to ensure good practice is understood and embedded into business as usual and that the right evidence 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 used right is Article 15, the right of access, which is 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. The Council's Information Governance Board has set the target that 85% of SARs should be answered in time.
4.4	In 2020/21, the Council handled 326 Subject Access Requests and answered 170 in time (see Appendix A). The overall SAR performance figure has dropped from 85% in 2019-20 to 52% in 2020-21. The drop in performance has been caused by the suspension of request handling in response to the COVID-19 pandemic.

4.5	In addition to the above, the ICO has corresponded with the Council on two separate occasions concerning Subject Access Requests received in 2020/21. The cases concerned situations where individuals complained to the ICO that they were not provided with the information to which they were entitled. The ICO has agreed with one complaint and required the Council to disclose information weekly to the data subject. In the other case, the ICO was satisfied that the Council responded appropriately to the request.
4.6	The handling of SARs remains a priority for the Council.
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 2020/21, the Council received 1543 requests and answered 64.64% in time (appendix B). This response rate is down from 93.25% in 2019/20 and fails to meet the Information Governance Board's target of response rate of 95% of requests answered in time.
5.4	The reduction in compliance is a direct consequence of the coronavirus pandemic. In Q1, we received almost half the number of requests typically received. By Q4, the number of requests rose to the same levels as before the pandemic. However, as demand stabilised, it has taken longer than normal to process requests because of the strain on resources across the Council caused by the pandemic. Work has taken place across portfolios to address the backlog and to improve the Council's compliance rates.
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 received 54 requests for Internal Reviews in 2020/21. In the case of 27, either the Council changed its position and released information or upheld the original decision, which was accepted by the requester. There are 27 Internal Reviews outstanding.
5.6	In addition to the above, the ICO has corresponded with the Council on nine separate occasions concerning FOI/EIR requests received in 2020/21. Of these nine cases, the Council resolved two informally with the customer and the ICO upheld two cases in favour of the Council. At the time of this report, five cases remain open and are either awaiting action by an ICO case officer or are awaiting formal closure.
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). In 2020/21, 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.
6.3	To date approximately 32 datasets have been published onto ESRI site and 12 datasets have been published on Data Mill North. Further work is required to encourage services within the Council 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 Information Commissioner's Office of the personal data breaches that have a high and ongoing risk to the data subjects affected.

7.2	In 2020/21, 262 incidents were logged through the Council's information security incident process; 109 of these incidents were classed as personal data breaches (see Appendix C1). Most of the breaches involved customer personal data and were caused by human error with emails or post being delivered to the wrong person. Of these breaches, eight 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 2020/2021, the Council made one application for Directed Surveillance that was granted by the Magistrate and has since been cancelled; the term 'cancelled', meaning that the period in which the Council is authorised to carry out the surveillance has expired.
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.
8.5	The Investigatory Powers Commissioner found that all recommendations arising from the 2017 inspection report have been fully addressed and discharged.
8.6	Recommendations were provided following the 2020 inspection; one recommendation relates to updating the RIPA policy and guidance which was last updated in 2018. A review is in place to update references to legislation, including a relevant social media policy section and a new list of approvers.
8.7	A new cycle of appropriate refresher training, including the new Chief Executive and all approvers was encouraged by the Commissioner and has now taken place. In addition, various messaging across the Council has been carried out to remind staff about RIPA best practice via e-learning, intranet bulletins and the circulation of the social media policy.
9.0	**INFORMATION GOVERNANCE RISK AND ISSUES**
9.1	In 2020/21, 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.
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.

	Technical protections in place have been strengthened significantly. As part of the Council's significant investment in Microsoft Technology it has taken advantage of Microsoft Security solutions including Exchange Online Protection and Microsoft Advanced Threat Protection to reduce the threats associated with email and protect our Windows 10 devices.
10.3	The Council's move from Windows 7 which is now unsupported by Microsoft to Windows 10 significantly improves the Council's cyber security stance.
10.4	Although the technical protection in place has improved over the period, the Council must be prepared to respond to any cyber security issue when it arises, and a potential Ransomware issue is of particular concern. To reduce the likely impact of such an issue, the Council has made a significant investment in new backup technology in line with guidance from the National Cyber Security Centre (NCSC) – migration to the new system (Rubrik) is currently in progress.
10.5	Over the period the Council has worked with 3rd party providers and central government security experts to assess ongoing areas of weakness. Despite the significant technical improvements made over the period some areas for improvement remain. It should be noted that the need to maintain services during the pandemic and provide IT service to people working at home is particularly challenging from a system management and security point of view, but to some extent the acceleration of the move to cloud based solutions such as Office 365 have enabled us to provide services remotely which would have been almost impossible to deliver at an affordable rate when the Council contracted its ICT to Capita.
10.6	The Council has recently implemented the use of data sensitivity labelling based on the government's information security classifications. The use of labelling has been a mandatory compliance requirement for authorities dealing with data provided by DWP via the Public Service Network (PSN) for more than 10 years. The implementation of labelling re-enforces the Council's IT estate was managed externally and brings Sheffield City Council belatedly in line with most other Councils and public bodies.
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 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 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 Information Management e-learning and Regulation of Investigatory Powers e-learning, which are available thought the Sheffield Development Hub. Bespoke training has also been available and delivered to officers needing greater knowledge in key 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. 88.98% of Council staff had completed the module by last month, with 96% of Social Care staff completing the training in time for the 2020/21 NHS Toolkit submission in June 2021.
12.4	Additionally, there has been training of discrete groups such as Foster Carers (11 sessions) student social workers (five sessions) and training with Place colleagues on Data Protection Impact Assessments, Privacy Notices, and Information Sharing Agreements. Some external training was commissioned for staff including the four Caldicott Guardians who are senior officers charged with the confidentiality of care records and their appropriate sharing, and eight others who support them. 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 processing.

Appendix A: FOI and EIR Requests Response Performance 2020/21

	Requests Received	Responses Issued			Responses Issued which were issued within 20 days	Responses Issued which were overdue
		Within 20 days	Overdue	Total		
Quarter 1	264	60	21	81	**74.07%**	**25.93%**
Quarter 2	422	235	149	384	**61.20%**	**38.80%**
Quarter 3	402	270	167	437	**61.78%**	**38.22%**
Quarter 4	455	264	122	386	**68.39%**	**31.61%**
Full Year	**1543**	**829**	**459**	**1288**	**64.36%**	**35.64%**

Appendix B-1: Subject Access Request Performance 20/21

2020/21	Received	Answered in time	Answered Late	In Progress in time	In Progress, but late	Compliance %
Qtr 1	63	27	36	0	0	**43**
Qtr 2	80	38	39	0	3	**48**
Qtr 3	69	41	22	0	6	**59**
Qtr 4	114	64	36	0	14	**56**
Total	326	170	133	0	23	**52**

Year	Received	Answered in time	Answered Late	In Progress in time	In Progress, but late	Compliance %
2017/18	192	94	98	0	0	49
2018/19	297	219	78	0	0	74
2019/20	343	295	48	0	9	86
2020/21	326	170	133	0	23	52

Appendix C: Reported Information Security Incidents and Personal Data Breaches

C-1 Quarterly Figures

	No. of Incidents	Personal Data Breaches	ICO Notified
2020-21	**262**	**109**	**8**
Q1	**51**	**29**	**4**
Corruption or inability to recover information	1	0	0
Incorrect recipient of email	2	1	0
Information disclosed in error (email, posted, fax, verbal)	35	20	2
Lost or stolen paperwork	3	1	1
Online Disclosure (e.g., website, social media)	5	5	1
Unauthorised access to IT systems	5	2	0
Q2	**55**	**33**	**4**
Cyber Attack (e.g., virus, ransomware, phishing email)	1	1	0
Incorrect recipient of email	1	1	0
Information disclosed in error (email, posted, fax, verbal)	38	23	2
Lost in transit or away from the office	1	0	0
Lost or stolen hardware	2	1	0
Online Disclosure (e.g., website, social media)	3	2	0
Other - non-encrypted personal data sent be email.	1	0	0
Unauthorised access to IT systems	2	2	2
(blank)	8	5	0
Q3	**67**	**29**	**0**
Cyber Attack (e.g., virus, ransomware, phishing email)	1	0	0
Information disclosed in error (email, posted, fax, verbal)	57	26	0
Lost or stolen hardware	3	0	0
Lost or stolen paperwork	1	0	0
Online Disclosure (e.g., website, social media)	1	1	0
Unauthorised access to IT systems	1	1	0
Unauthorised access to physical documents	3	1	0
Q4	**89**	**18**	**0**
Cyber Attack (e.g., virus, ransomware, phishing email)	1	0	0
Information disclosed in error (email, posted, fax, verbal)	74	16	0
Lost or stolen hardware	1	0	0
Lost or stolen paperwork	3	0	0
Online Disclosure (e.g., website, social media)	3	1	0

	No. of Incidents	Personal Data Breaches	ICO Notified
Unauthorised access to IT systems	4	0	0
Unauthorised access to physical documents	3	1	0

C2 – Summary of personal data breaches investigated by the ICO

SCC Ref.	Incident reported	Summary of the personal data breaches investigated by the Information Commissioner's Office	INCIDENT TYPE
2020-258	24/04/20	ANPR data consisting of 8.6 million vehicle registration numbers, and the associated date, time and location of vehicle was available on the Internet. The ICO issued a reprimand to the council for a lack of control and overall governance of the ANPR system. It welcomed the remedial steps taken by SCC: access to the ANPR system was removed, data controllership of the ANPR system was established and a full audit of the ANPR system was completed.	Unauthorised access to IT systems
2020-265	11/05/20	During the pandemic, the collection of council tax debt from individuals had been suspended. Individual single page notifications to the DWP and employers to suspend deductions from benefits or cease attachment of earnings were printed double-sided and automatically enveloped. That meant that employers received notifications of their own employee and that of another employer, breaching that individual's confidentiality. 144 data subjects were affected (although 556 other individuals were double-sided printed in the notification to the DWP. This information was considered contained by a trusted partner.)	Information disclosed in error [Both incidents were bundled into a single notification because they related to the same issue close to each other]
2020-284	17/06/20	An earlier incident involving business rate debt recovery suspension with the breach of the personal data of 17 sole traders. Requested recipients destroy original letters which were all replaced; data subjects were informed and apologised to; processes were tightened; and training arranged. The ICO took no further action following several recommendations of good practice.	
2020-271	19/05/20	Social worker's bag stolen from car whilst visiting a client, containing mobile phone, tablet, notebook, diary, and daily tasks book. Extensive measures were taken to contain the incident. The ICO closed the case with no further action and made several recommendations.	Lost in transit or away from the office
2020-278	5/06/20	Information was published on SCC website for the Admissions Committee which considers appeals for school placements, where it remained for 48 hours. The agenda pack included confidential documents and was meant only for those Council Members on the committee. The council took action to retrieve the information and support the families. The ICO closed the case with no further action but made several recommendations.	Information disclosed in error
2020-330	14/08/20	An allegation was received from a member of the public that confidential information from council records had been posted to Facebook. The case was not proved. The ICO closed the case.	Unauthorised access to IT systems

SCC Ref.	Incident reported	Summary of the personal data breaches investigated by the Information Commissioner's Office	INCIDENT TYPE
2020-331	20/08/20	In response to a conversation with a tenant regarding an ongoing anti-social behaviour case, the officer posted several diary sheet templates and a compliment slip to the wrong address. The data subject was informed and apologised to, and processes tightened. The ICO closed the case with a few recommendations.	Information disclosed in error
2020-336	27/08/20	A member of staff accessed records regarding an anti-social behaviour complaint made against them. The ICO closed the case based on actions taken by the council; and reiterated good practice.	Unauthorised access to IT systems
2020-339	4/09/20	The incident related to the disclosure of exam grades in a tribunal hearing, revised due to pandemic moderation, and until that point unknown to the individual concerned who was distressed by what they considered a breach of confidentiality. The ICO closed the case with a couple of recommendations.	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?	1
	The number of Directed Surveillance authorisations successfully granted?	1
	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?	1
	The number of Directed Surveillance authorisations extant at the end of the year?	0

This page is intentionally left blank