Classification: Public

Key Decision: No

Gravesham Borough Council

Report to: Performance & Administration Cabinet Committee

Date: 20 Sept 2023

Reporting officer: Sarah Parfitt, Director (Corporate Services)

Subject: Information Governance Annual Report: 2022-2023

Purpose and summary of report:

This report is intended to provide Members of the Performance & Administration Committee, (whose terms of reference includes information governance) with an overview of the current arrangements within the council to strategically manage information, including compliance with key standards.

Recommendations:

1. This is an information only report.

Key Implications:	
Item	**Implications**
Legal	The Information Governance activity of the council is directed by a number of pieces of legislation. This report is intended to provide Members with information on compliance with key legislation and broader information governance compliance.
Finance and Value for Money	There are no financial or value for money implications arising from this report.
Corporate Plan	#3: Progress: an entrepreneurial authority; commercial in outlook and committed to continuous service improvement, underpinned by a skilled workforce and strong governance environment.
Climate Change	There are no direct climate change impacts from the information governance activity carried out by the council, however the way the council holds and stores data can contribute to the pledge of the council to work towards being carbon neutral by 2030.

1. Introduction

1.1 The term Information Governance relates to the framework to support legal compliance, transparency and risk management in managing information managed and handled by the council in whatever medium it is held, balancing these requirements against the objectives of the council to deliver effective services.

1.2 The Senior Information Risk Owner (SIRO) has overall responsibility for managing information risk in the council and chairs the Information Governance Strategy Group. The SIRO is the Director (Corporate Services) who has responsibility to:

- foster a culture for protecting and using information within the council
- ensure arrangements are in place to deliver information governance compliance with legislation and council policies
- provide a focal point for managing information risks and incidents
- prepare an annual information risk assessment for the council.

1.3 The Assistant Director (IT & Transformation) is designated as the Deputy Senior Information Risk Officer.

1.4 By working alongside Cabinet, Management Team, the Data Protection Officer (DPO), the Information Governance Team, IT and other key stakeholders, the SIRO aims to create a culture in which information is valued as an asset and information risk is managed in a realistic and effective manner.

Diagram of SIRO relationships with officers across the Council

1.5 It is vital that the SIRO engages with the above stakeholders across the Council, to ensure a “golden thread” of good information governance combined with the corporate oversight.

2. Information Governance Management Framework

2.1 Gravesham Borough Council's Code of Corporate Governance states:

"*Governance is about how authorities ensure they are providing the right services to the right people in a timely, open, honest and accountable manner*."

2.2 It is essential that the council has a robust information governance management framework, to ensure that information is effectively managed with accountability structures, governance processes, documented policies and procedures, staff training and adequate resources.

2.3 Since 2016 the council has operated a shared service arrangement, hosted by Medway Council, to provide resource to support its Information Governance arrangements.

2.4 To ensure the council meets the requirements of the code, the Information Governance Manager has developed the council's Information Governance Management Framework. This is available to all officers and members via the intranet.

2.5 This framework and the supporting standards will be monitored and reviewed bi-annually in line with legislation and codes of best practice. The next review will be discussed at the Information Governance & Security Group (IGSG) meeting in November 2023.

3. Policy Review

3.1 The Information Governance Team has developed a suite of policies intended to provide the principles by which its information governance arrangements will be directed. These policies are reviewed on at least a bi-annual basis for consideration and approval by the Information Governance Strategy Group and Management Team. Where there is release of new national guidance or legislation, policies are created/amended to reflect this. The current timetable for policy review is as follows:

Policy Title	Review Date
Data Protection Policy	January 2025
Subject Access Request	March 2025
Data Breach Policy	Sept 2023
Information Sharing Policy	January 2024
Records Management Policy	November 2023
Anonymisation and Pseudonymisation Policy	March 2024

4. Freedom of Information and Environmental Information Requests

4.1 The Freedom of Information (FOI) Act 2000 provides the ability for members of the public to request information from public authorities. The Environmental Information (EIR) Act 2004 provides the ability for members of the public to request environmental information from public authorities.

4.2 The next table below shows the number of FOI and EIR requests received by the council during 2022-2023.

Period	FOI & EIR Requests received 2022-23	% of responses within 20 working days 2022-23
Q1	133	84%
Q2	125	94%
Q3	118	99%
Q4	161	93%
	537	**93%**

4.3 The expected rate set by the ICO for response (within 20 working days) to FOI & EIR is above 90%. The council has kept its performance above expected rate as of Q2 with 93% requests responded within 20 working days on average.

5. Subject Access Requests

5.1 Under Data Protection legislation, an individual can make a Subject Access Request (SAR) to obtain a copy of their personal data being processed by an organisation. The table below shows the number of SARs received by the council during 2020-21 and 2021-2022.

Number of SARs received 2022-23	% of responses within 30 days 2022-23
17	76%

5.2 The GDPR law has set a deadline to respond to Subject Access Requests within 30 days (or 1 calendar month). An extension of further 60 days can be requested if the request is of complex nature. 76% requests were responded within deadline in 2022-23. The council identified the need for SAR policy which was approved and implemented in Q1 2023 and is available to all staff via Staff Intranet.

5.3 Training to support officers involved in handling SARs was also delivered during 2022/23. The Information Governance team and the DPO continues to provide support and guidance to the council ensuring SARs are handled and responded as per the guidelines set in the GDPR law.

6. Data Incidents

6.1 A data incident is defined as any event that results, or may result, in the potential for unauthorised access to, loss or destruction of personal data.

6.2 During 2022-23, the council recorded 15 data incidents; none of which met the threshold for reporting to the ICO. This compares to 9 data incidents in 2021-22.

6.3 The Information Governance Team has developed a Case Management register to facilitate identification of risks and trends to inform any mitigation measures required. All data incidents must be recorded on Case Management regardless of

whether these are reported to the ICO or not. This is a mandatory requirement stated under Article 33 of the UK GDPR law.

6.4 Data incidents are reviewed by Data Protection Officer and Senior Information Risk Owner and where considered appropriate, training advice or reminders are issued to staff to remind them of their responsibilities regarding the protection of personal data. Trends in data incidents are also monitored by the Information Governance Strategy Group each quarter so that these can be understood, and action taken at a corporate level if this is required.

6.5 One of the key steps of data breach management process is to ensure learning from each incident is noted and any changes are implemented to reduce the risk of recurrence. One of the learning from the incidents that occurred in the year 2022-23 is to ensure Outlook auto-select/cache feature is regularly emptied to ensure auto select functionality doesn't cause automatic selection of the email recipient. Other learnings include use of document highlighting to update the text especially when using mail merge feature; and also, where the details are being entered on the system, a thorough search is conducted before information is updated to an existing database.

7. Publication Scheme

7.1 The Freedom of Information Act 2000 requires that every public authority has a Publication Scheme, which provides a reference point for members of the public to understand the information the council holds and the categories of information it will publish and make available. The ICO has created a model publication scheme that all public authorities must use.

7.2 The council's Publication Scheme was reviewed during 2021, with the revised Publication Scheme placed on the council website.

8. Surveillance Camera Local Authority Code of Practice

8.1 The council is responsible for ensuring that each surveillance camera system that it operates has a clearly defined purpose; considers the effect that their use has on individuals and their privacy; and, that they are operated in a manner which meets the council's statutory responsibilities and complies with the Surveillance Camera Commissioner's Code of Practice.

8.2 The Council's adopted its Surveillance Camera Local Authority Code of Practice in March 2022.

9. Training

9.1 Training forms a key part of maintaining the council's Information Governance arrangements.

9.2 During 2022-23 the Subject Access Request training was delivered to officers involved in responding to such requests, alongside Data Protection Training for officers via an online training platform.

9.3 An informal training/awareness session was held by Information Governance Manager where a data breach was reported and upon investigation, it was identified that the team requires further awareness in handling personal data.

10. Looking Forward

10.1 The council will continue to undertake activity to maintain, develop and enhance its information governance arrangements. The following sets out the main priorities for the Information Governance Team over the next year:

11. Summary

11.1 Good Information Governance enables officers and Members to perform their roles in a supportive way whilst ensuring they remain compliant, provide the necessary safeguards to protect personal information, are proactive in storing, managing and eventually destroying information in line with the retention schedule and do all of these in a secure way.

11.2 The public need to trust that the council are taking its role as guardian of their information seriously and the council can provide that reassurance by having robust and resilient systems and processes in place. The SIRO and the Information Governance team will continue to support, advise, challenge and question the working practices of services. The benefits of doing this will lead to staff being more confident and empowered in managing information and contribute to the successful delivery of business goals through teams having the right information to focus on the most effective solution to service provision.

11.3 The 2023 National Risk Register has included cyber threats as one of nine themes which would have a substantial impact on the UK's safety, security and/or critical systems at a national level. The councils Corporate Risk Register recognises this, and prioritises mitigations.

11.4 A proactive and multi layered approach is taken to address cyber security threats which includes regular staff awareness and training, technical controls (such as firewalls and anti-virus software) and data backup and recovery arrangements.

11.5 The proactive areas also include continual risk assessment, regular threat scanning, and continuous improvement (including services made available by the National Cyber Security Centre Active Cyber Defence programme).

11.6 The ability to deliver services depends on the ability to have safe systems and reliable information.

11.7 The IT and Digital Strategy 2022-2026 has highlighted the continual improvement of Cyber Security as a key objective.

Lead Officer: Sarah Parfitt, Senior Information Risk Owner and Director (Corporate Services)

Email: sarah.parfitt@gravesham.gov.uk

Secondary Implications	
Risk Assessment	Ongoing review, maintenance and development of the council's information governance framework arrangements contributes to ensuring the robustness of the overall governance arrangements of the council.
Data Protection Impact Assessment	*A data protection impact assessment (DPIA) should be carried out at the start of any major project involving the use of personal data or if you are making a significant change to an existing process.*
	a. Does the project/change being recommended through this paper involve the processing of personal data or special category data or criminal offence data? A definition of each type of data can be found on the Information Commissioner's Office website via the above links. N/A
	b. If yes to question a, have you completed and attached a DPIA including Data Protection Officer advice? N/A
	c. If no to question b, please seek advice from your nominated DPIA assessor or the Information Governance Team at gdpr@medway.gov.uk. N/A
Equality Impact Assessment	a. Does the decision being made or recommended through this paper have potential to cause adverse impact or discriminate against different groups in the community? If yes, please explain answer. N/A
	b. Does the decision being made or recommended through this paper make a positive contribution to promoting equality? If yes, please explain answer. N/A
	In submitting this report, the Chief Officer doing so is confirming that they have given due regard to the equality impacts of the decision being considered, as noted in the table above
Crime and Disorder	No direct implications.
Digital and website implications	The council is required to publish certain types of information and maintain a Publication Scheme to enable members of the public to understand the information the council holds and the categories of information it will publish. The council website is used for these purposes.
Safeguarding children and vulnerable adults	Strong information governance can contribute to safeguarding activity.