Public report

Audit and Procurement Committee   29 January 2025

Name of Cabinet Member:
Cabinet Member Policy and Leadership - Cllr G Duggins

Director approving submission of the report:
Director of Law and Governance

Ward(s) affected:
N/A

Title:

Information Governance Annual Report 2023/2024

_____

Is this a key decision?
No

_____

Executive summary:

Information is one of the Council's greatest assets and its correct and effective use is a major responsibility and is essential to the successful delivery of the Council's priorities. Ensuring that the Council has effective arrangements in place to manage and protect the information, both personal and business critical, it holds is a priority.

Data protection legislation sets out the requirements on organisations to manage information assets appropriately and how they should respond to requests for information. The Information Commissioner's Office (ICO) is the UK's independent supervisory authority set up to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals, and monitors compliance with legislation.

This report provides a summary of the Council's performance during 2023/2024 in responding to requests for information received under the above-mentioned legislation. It also reports on the management of data protection security incidents and/or those reported to the ICO and data protection training.

Recommendations:

The Audit and Procurement Committee is recommended to:

1) Note the Council's performance on Freedom of Information, Subject Access and other Data Protection Act requests, including the outcomes of internal reviews and the number and outcome of complaints made to the ICO.
2) Note the reporting and management of data security incidents.
3) Note data protection training compliance.
4) Identify any comments or recommendations.

List of Appendices included:
None

Background papers:
None

Other useful documents
None

Has it or will it be considered by Scrutiny?
No

Has it or will it be considered by any other Council Committee, Advisory Panel or other body?
No

Will this report go to Council?
No

Report title: Information Governance Annual Report 2023/2024

1.   Context (or background)

1.1   Information Governance (IG) is the strategy or framework for handling personal information in a confidential and secure manner while ensuring compliance with the relevant statutory and regulatory requirements. IG within the Council is delivered through a distributed model of responsibility rather than through the sole responsibility of the IG Team, with key roles identified and assigned to ensure appropriate oversight and accountability:

- Head of Information Governance
- Information Governance Team
- Senior Information Risk Officer (SIRO)
- Data Protection Officer (DPO)/DPO Team
- Caldicott Guardian
- Information Asset Owners (IAO)
- Information Asset Managers (IAM)
- Information Management Strategy Group

1.2   The function of Information Governance supports the Council's compliance with the UK General Data Protection Regulations GDPR (UK GDPR), Data Protection Act (DPA) 2018, Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations (EIR). The Council has a statutory obligation to comply with the IG framework by responding appropriately to requests and managing personal data lawfully. The IG Team assist the organisation by monitoring internal compliance, informing and advising on data protection obligations, providing advice and guidance and raising awareness on data protection matters.

1.3   The FOIA and EIR impose a statutory obligation on the Council to respond to requests for information within 20 working days, subject to relevant exemptions. The Code of Practice, issued by the Secretary of State for Constitutional Affairs under Section 45 of the FOIA, requires public authorities to have a procedure in place to deal with complaints in regard to how their requests have been handled. This process is handled by the Information Governance Team as an FOI or EIR internal review. After an internal review has been completed an applicant has a right to complain to the Information Commissioner's Office (ICO) for an independent ruling on the outcome. Based on the findings of their investigations, the ICO may issue a Decision Notice. The ICO may also monitor public authorities that do not respond effectively and in a timely manner to the FOI/EIR requests they receive and may take enforcement action or issue reprimands accordingly.

1.4   The DPA 2018 provides individuals with the right to ask for information that the Council holds about them. These are also known as Subject Access Requests (SARs). The Council should be satisfied about the individual's identity and have enough information about the request. The timescale for responding to these requests is one month, starting on the day of receipt. Authorities can extend the time taken to respond by a further two months if the request is complex or a number of requests have been received from the individual, e.g. other types of requests relating to individuals' rights.

1.5   There is no requirement for the Council to have an internal review process for SARs. However, it is considered good practice to do so. Therefore, the Council informs

applicants of the Council's internal review process. However, individuals may complain directly to the ICO if they feel their rights have not been upheld.

1.6   The Council also receives one-off requests for personal information from third parties including the police and other government agencies. The IG Team maintains a central log that includes exemptions relied on when personal data is shared with third parties. They provide advice and assess whether the Council can lawfully disclose the information or not.

1.7   The Council's management of data protection security incidents is undertaken by the Data Protection Officer Team, they record, investigate and where necessary, recommend actions to be taken based on the impact risk level.

1.8   The Data Protection Officer Team supports the Council in understanding the impact of plans, projects and activities on data protection through a process of impact assessments to support decision-making. The Council also has arrangements in place to support the sharing of data where appropriate and the team provide support in the preparation and sign off of on-going and one-off data sharing agreements.

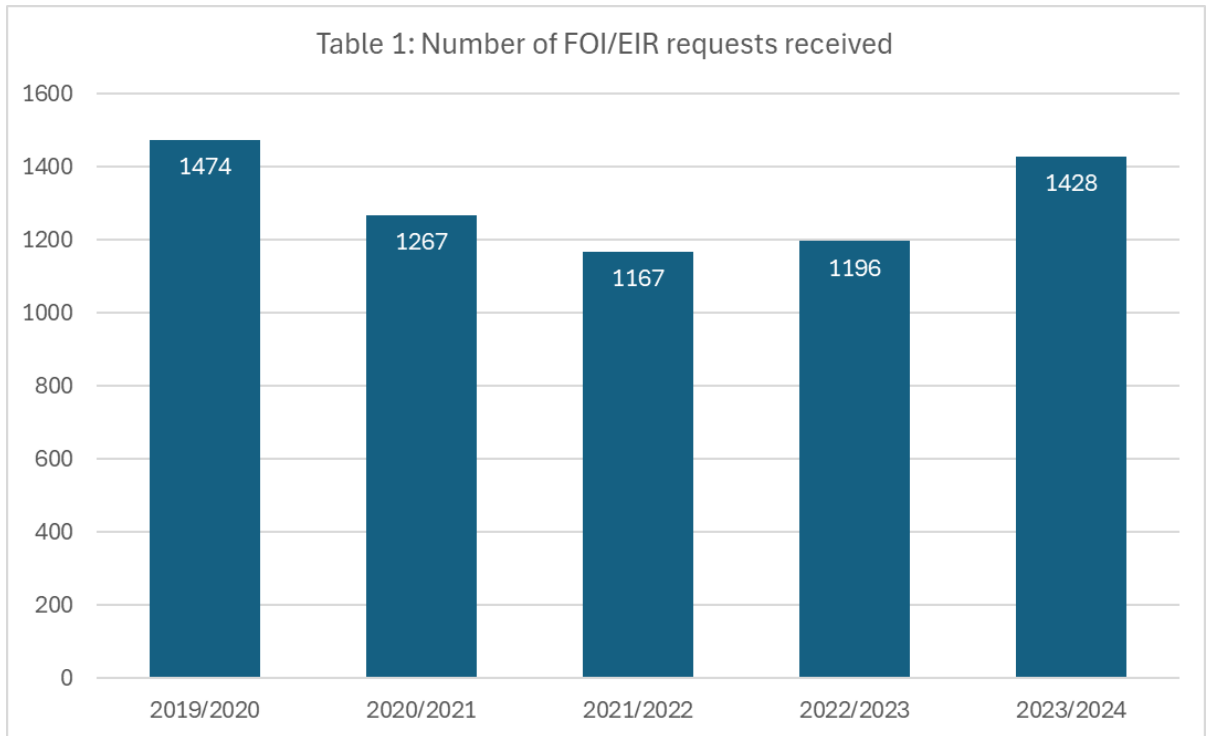## 2.   Information Governance Annual Report 2023-2024

2.1   Context

2.1.1   The landscape in which public authorities are now operating has continued to change since the introduction of the GDPR and subsequently UK GDPR and the Data Protection Act 2018 (DPA 2018) in 2018.

2.1.2   This landscape will continue to change. Good information governance has an important part to play as the introduction of integrated care systems has brought partnerships of organisations together to plan and deliver joined up health and care services, and to improve the lives of people who live and work in their area and effective cyber security is an increasingly key element in protecting and preventing unauthorised access to personal information. The development of Artificial Intelligence provides opportunities as well as risks in relation to the use of data and is addressed both in the proposed changes to legislation and the Council's developing approach.

2.1.3   In March 2023, the Government introduced the Data Protection and Digital Information Bill which did not complete its passage through parliament prior to the UK parliamentary general election being called for July 2024. The new Government has subsequently introduced to parliament the Data (use and Access) Bill with the stated purpose to "unlock the secure and effective use of data for the public interest". While it retains some of the measures proposed in its predecessor, others are amended and some new elements introduced. Implications for local government will be monitored as the Bill progresses to ensure that the City Council is able to meet the new requirements when they are introduced.

2.1.4   In June 2022, the ICO set out a revised approach to working more effectively with public authorities. This approach has seen an increased use of the ICO's wider powers under data protection law, including warnings, enforcement notices and

reprimands as well as changing its approach to the application of fines in the public sector and the ICO is currently considering the next steps.
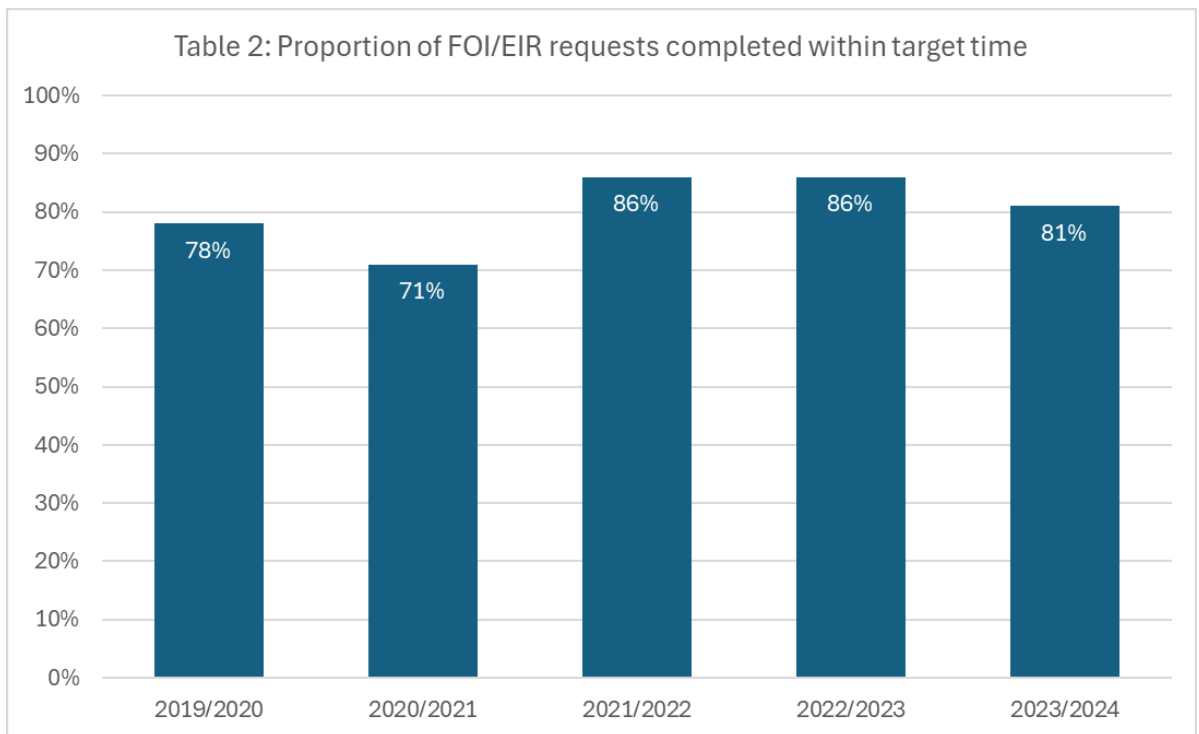
2.2   Requests for Information

2.2.1   The number of Freedom of Information Requests received by the Council in 2023/24, 1428 was an increase of 232 requests on the previous 2022/23 year. The Council responded to 81% of FOIA/EIR requests within the target time of 20 working days in 2023/24 which was a decrease on the previous year (see table 2). This is below the 90% threshold set by the ICO.

2.2.2   The Council received 30 requests for internal reviews in the year 2023/24 (down from 37 the previous year). The Council responded to these with the following outcomes:
- 10 were not upheld – the exemptions that had been applied were maintained and no further information was provided;
- 6 were not upheld – but advice or clarification was provided;
- 4 were partially upheld – some further was information provided;
- 7 were upheld - information was provided;
- 3 were withdrawn.

2.2.3   The City Council already publishes a significant amount of information and is identifying opportunities to increase the volume and type of information published (subject to legal compliance). This will increase transparency and help to reduce the number of FOI's the Council receives because the information will already be available.

2.2.4   No complaints were made to the ICO during 2023/24 (compared to 12 the previous year).

Table 1. Number of FOI/EIR requests received

Table 1: Number of FOI/EIR requests received

Year	Requests
2019/2020	1474
2020/2021	1267
2021/2022	1167
2022/2023	1196
2023/2024	1428

Table 2. Proportion of FOI/EIR requests completed within target time

Table 2: Proportion of FOI/EIR requests completed within target time

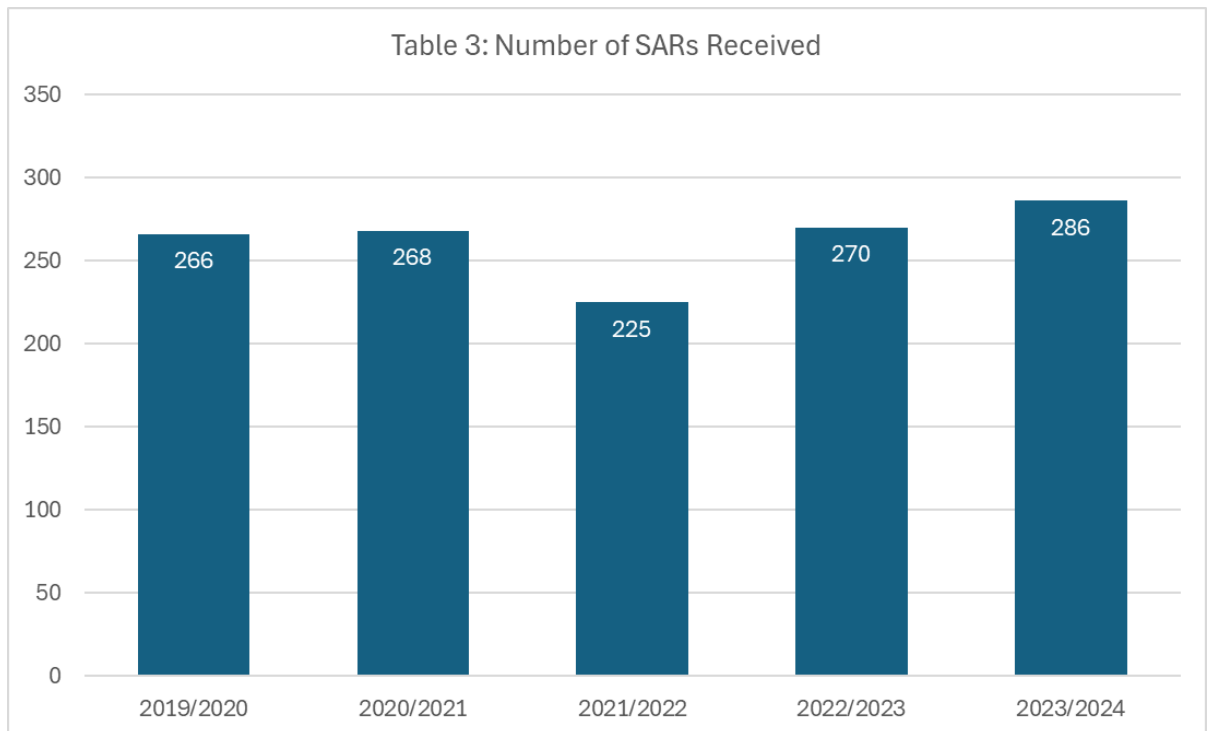| Year	Proportion
2019/2020	78%
2020/2021	71%
2021/2022	86%
2022/2023	86%
2023/2024	81%

2.2.5   286 valid Subject Access Requests (SARs) were received during 2023/24, an increase of 13 on the previous year (see table 3). While the Council receives fewer SARs than other information requests, many of these are complex and can involve managing significant amounts of sensitive information. The number of requests relating to Children's Social care, as well as the number of SARs to which extensions were

applied due to their size and/or complexity both increased significantly. The completion rate within the target time increased to 84% in 2023/24 (up from 79% the previous year (see table 4).

2.2.6   The Council received 12 requests to carry out an internal review into a SAR application during 2023/24, the same number as in the previous year. In 9 cases, further information was provided which was located through further searches based on information provided by the requester or by reviewing the information which had originally been redacted. Where information was not provided, this was due to the original exemptions being upheld or information not being held by the Council.

2.2.7   No complaints were made to the ICO related to Subject Access Requests in 2023/24.

Table 3. Number of SAR's received

Table 3: Number of SARs Received

Table 4. Proportion of SARs responded to within target time

Table 4: Proportion of SARs responded to within target time

Year	Percentage
2019/2020	79%
2020/2021	86%
2021/2022	79%
2022/2023	77%
2023/2024	84%
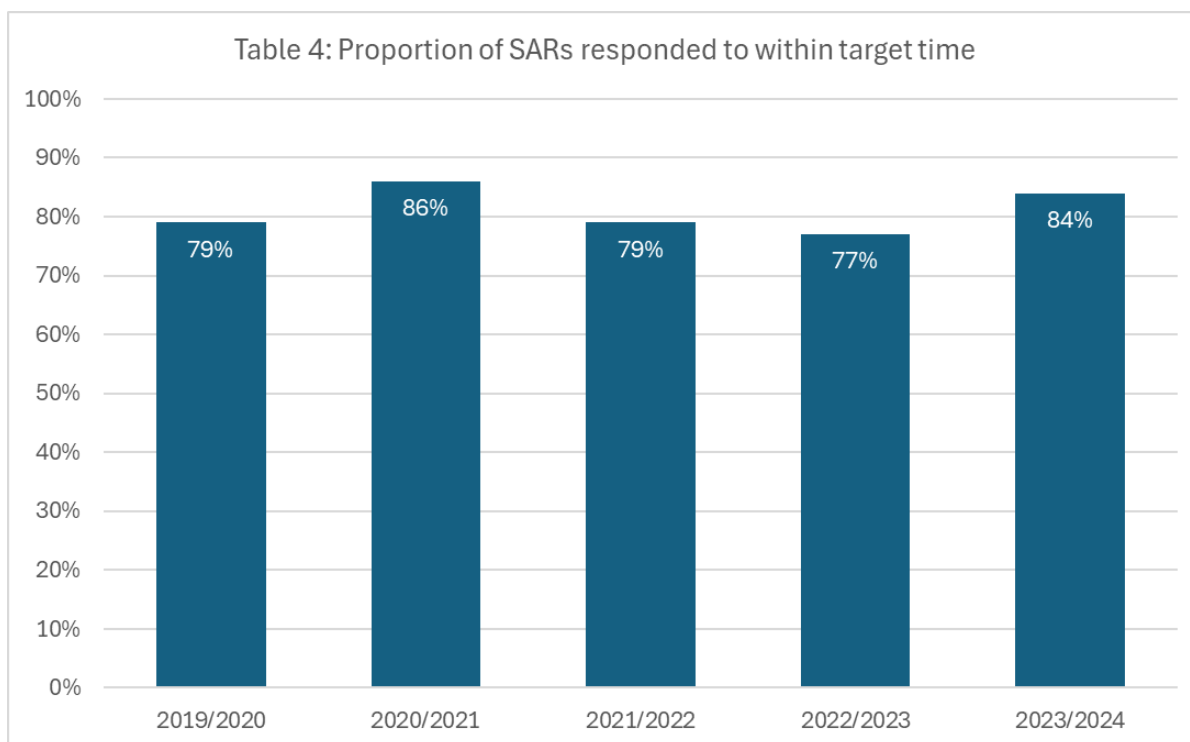
2.3 Data Security Incidents

2.3.1 Protecting information from theft, loss, unauthorised access, abuse and misuse is crucial in order to reduce the risk of data breaches or financial loss incurred through non compliance with key legislation.

2.3.2 The IG data protection security incident reporting process supports the Council's objective that breaches are managed promptly, and outcomes of investigations are used to inform reviews of the control measures in place to keep personal information secure.

2.3.3 In addition, the Council actively encourages the reporting of near misses and potential breaches to identify learning, promote awareness and reduce the likelihood of a serious breach to information even though not all reported incidents will have resulted in a breach. Even where there is no breach, incidents can provide valuable insight into training requirements and processes and procedures which may need to be strengthened as a preventative measure. When investigating data protection security incidents, the Data Protection Team routinely consider resultant training needs and provide advice and guidance as required. Messages continue to be provided to staff alerting them to the need to protect personal data and use it appropriately.

2.3.4 In 2023/24, 176 reports of information security incidents were sent to the Data Protection Team, a decrease from 219 in the previous year. Of these, 103 did not involve a breach of personal data. These included for example near misses, loss or theft of equipment, cases where technical measures prevented access to data and incidents where a breach was contained. Of the incidents where a breach of personal

data was identified, 70 were identified as low risk, 1 medium and 1 high. The majority of reports were classified as information being disclosed in error (75) with 57 reports relating to technical/procedural errors, 28 reports relating to loss or theft of hardware and one to unauthorised access.

2.3.5 The GDPR introduced requirements for personal data breaches that meet certain thresholds to be reported to the ICO. Two self-reports were made to the ICO during 2022/2023.

2.3.6 One complaint was made to the ICO during 2023/2024 related to the council's Data Protection Obligations. The ICO confirmed that they did not intend to take regulatory action and provided guidance to the council on measures to implement to avoid future incidents.

2.4 Training and Awareness

2.4.1 Data Protection training is key to ensuring staff are aware of their responsibilities. Training is currently delivered through the Council's e-learning platform and annual completion of the data protection course is mandatory for all staff with access to personal data. Staff who do not have access to a computer in their role (not office based) and those with minimal personal data involved in their role are provided with appropriate level training. This ensures that an appropriate level of understanding and awareness is reached that is relevant to their role/responsibilities.

2.4.2 The data protection training strategy is kept under review and updated as required. New cyber security training is being introduced to replace the existing information security training and reflect the changing environment in which the Council operates. Other information and awareness raising is undertaken throughout the year in response to local and national issues. For example, ICT have delivered awareness sessions specifically relating to cyber security and regular cyber security messages are issued by ICT to staff. This has included a programme of awareness raising during cyber security month.

2.4.4 For the 2023/24 year, the Council reported a completion rate of the Council's mandatory data protection training of 95%. The Elected Member Training and Development Strategy, introduced for the 2022/2023 year, also includes data protection training.

2.5 Data Security and Protection and Toolkit

2.5.1 The Data Security and Protection Toolkit is an online tool that allows relevant organisations that process health and care data to measure their performance against data security and information governance requirements which reflect legal rules and Department of Health policy. This self-assessment tool enables the Council to demonstrate that it can be trusted to maintain the confidentiality and security of personal information, specifically health and social care personal records.

2.5.2 All organisations that have access to NHS patient data and systems use this Toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly.

2.5.3 For the 2023/24 reporting period, the Council met all of the mandatory requirements and was assessed as meeting required standards.

3.   Options considered and recommended proposal

3.1   The recommended proposal is that Audit and Procurement Committee consider and note the Annual Report. In addition, the Committee is recommended to forward any comments or recommendations to the Cabinet Member Policy and Leadership.

3.2   The only other option is to "Do Nothing" which is not recommended as it is essential that the Council continues to monitor and report on its performance in relation to access to information requests, information security incidents and training completed in order to promote best practice information governance and drive continuous improvement in the Council's ability to comply with the laws relating to information.

4.   Results of consultation undertaken

4.1.   None

5.   Timetable for implementing this decision

5.1.   Not Applicable

6.   Comments from Director of Finance and Resources and Director of Law and Governance

6.1.   Financial Implications
       There are no specific financial implications resulting from the issues within this report although it is worth noting that the Information Commissioner's Office is able to levy significant fines for serious non-compliance with the legislation surrounding the management of information.

6.2.   Legal Implications
       There are no specific legal implications arising out of the recommendations. However, the Council's performance is subject to external scrutiny by the ICO, who have the authority to impose sanctions upon the Council for non-compliance. The monitoring and reporting on the outcomes of ICO complaints represents good practice and promotes good governance and service improvement.

7.   Other implications

7.1. **How will this contribute to the One Coventry Plan?**

The monitoring and reporting of the Council's performance regarding responding to, and handling access to information requests under FOIA and DPA 2018, including any complaints made to the ICO will enable continuous improvement, raise awareness and promote high standards of information governance, fostering a culture of openness and transparency within the Council and demonstrating our commitment to best practice information governance, security, and protection.

7.2. **How is risk being managed?**

The reporting and monitoring on the Council's performance to information laws and outcomes of ICO complaints will help protect information and reduce the risk of the ICO upholding complaints and taking enforcement action against the Council.

7.3. **What is the impact on the organisation?**

Operating best practice Information Governance and Security will support public confidence in the Council, offering assurance to service users of the council's commitment to Data Protection and Transparency. Partner and client organisations will have the assurance they required in order to engage with the Council and share data. The risks of serious breaches of personal Data/Information Assets should be reduced, protecting information and reducing the likelihood of action by the ICO.

7.4. **Equalities / EIA?**

The Council's responsibilities under Section 149 of the Equality Act 2010 are supported by UK GDPR/DPA 2018, requiring that Special Category Data is afforded extra measures of security to protect that data. .

7.5. **Implications for (or impact on) climate change and the environment?**

None

7.6. **Implications for partner organisations?**

As set out in paragraph 7.3 above.

Report author(s):
Adrian West
Head of Governance / Data Protection Officer

Service Area:
Information Governance

Telephone and email contact:
Tel: 024 7697 1007
Email: adrian.west@coventry.gov.uk

Enquiries should be directed to the above person

Contributor/approver name	Title	Service Area	Date doc sent out	Date response received or approved
Contributors:				
Lara Knight	Governance Services Officer	Law and Governance	13/01/25	17/01/25
Sue Gilbert	Information Governance Officer	Law and Governance	13/01/25	15/01/25
Preeti Mistry	Information Governance Officer	Law and Governance	13/01/25	15/01/25
Rebecca Newstead	Information Governance Officer	Law and Governance	13/01/25	15/01/25
Names of approvers for submission: (officers and members)				
Finance: Richard Shirley		Finance	13/01/25	21/01/25
Legal: Amy Wright	Regulatory Services Team Leader	Law and Governance	13/01/25	15/01/25
Director: Julie Newman	Director of Law and Governance	-	13/01/25	16/01/25
Members: Cllr G Duggins	Leader and Cabinet Member for Policy and Leadership	-	13/01/25	16/01/25

This report is published on the council's website: www.coventry.gov.uk/meetings