Coventry City Council

Public report

Audit and Procurement Committee — 21 September 2026

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

Director approving submission of the report:
Director of Law, Governance and Safer Communities

Ward(s) affected:
N/A

Title: Information Governance Annual Report 2025/2026

Is this a key decision?
No

Executive summary:

Information is one of the Council's most important assets. Its proper and effective use is essential to the successful delivery of the Council's priorities and is a key organisational responsibility. Ensuring that robust arrangements are in place to manage and protect the personal and business-critical information held by the Council remains a priority.

Data protection legislation sets out how organisations must manage information assets and respond to requests for information. The Information Commissioner's Office (ICO), as the UK's independent supervisory authority, upholds information rights in the public interest, promotes openness by public bodies and data privacy for individuals, and monitors compliance with relevant legislation.

This report provides a summary of the Council's performance during 2025/2026 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 2025/2026

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:

- Information Governance Manager
- 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 data protection legislation including the UK General Data Protection Regulations GDPR (UK GDPR), Data Protection Act (DPA) 2018, the Data (Use and Access Act) 2025, 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 place a statutory duty on the Council to respond to requests for information within 20 working days, subject to the application of any relevant exemptions or exceptions. 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 for handling complaints about the way requests have been dealt with. Within the Council, this process is managed by the Information Governance Team as an FOI or EIR internal review. Once an internal review has been completed, the applicant has the right to complain to the Information Commissioner's Office (ICO) for an independent decision. Following its investigation, the ICO may issue a Decision Notice. The ICO may also monitor public authorities that fail to respond effectively or within statutory timescales to FOI/EIR requests and may take enforcement action or issue reprimands where appropriate.

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 The Data (Use and Access) Act 2025 requires Data Controllers to implement a Data Protection Complaints procedure by 19 June 2026. This provides individuals with the right to complain if they consider that the Council has infringed UK GDPR or part 3 DPA 2018, to include the handling of SARs, unauthorised or unlawful use of their data or concerns about data breaches or data security. Accordingly, the Council published its Data Protection Complaints procedure on 19 June.

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 2025-2026

2.1 Context

2.1.1 The operating environment for public authorities has continued to evolve since the introduction of the GDPR, followed by the UK GDPR and the Data Protection Act 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 to plan and deliver joined up health and care services continue to develop, the use of AI to transform service delivery develops and the cyber security landscape becomes more challenging.

2.1.3 Since 2023, successive governments have proposed legislation to reflect the changing context in which personal data is managed. The Data Use and Access Act 2025 (DUAA) received Royal Assent in June 2025 and introduced targeted reforms to the UK's data protection framework. It amends aspects of both the UK GDPR and DPA 2018 whilst retaining the core data protection principles. It provides better clarity about what constitutes a reasonable and proportionate search for a SAR and strengthens data sharing provisions when required to support a public task.

2.1.4 The ICO continues to apply its revised approach to working more effectively with public authorities initially introduced in June 2022. 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. The DUAA establishes a new strategic framework for the ICO to focus on public trust, innovation and competition as well as upholding data protection, changing its governance model to become the Information Commission with an executive and board of directors and expanded powers and regulatory oversight.

2.2 Requests for Information

2.2.1 The number of Freedom of Information Requests received by the Council in 2025/26 was 1,454, which was an increase on the number of requests received in the previous year (see table 1). The Council responded to 80% of FOIA/EIR requests within the target time of 20 working days in 2025/26 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 27 requests for internal reviews in the year 2025/26 (down from 37 the previous year). Of the 27 requests for internal review received, 15 upheld the use of an exemption in the initial response, 3 clarified the earlier response and 8 provided further information. One was not accepted as was made out of time.

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 Three complaints were made to the ICO on FOI/EIR related matters during 2025/26 (compared to four the previous year). In one case, the ICO has issued a decision notice which upheld the exemption the Council had applied but found that the Council had not provided appropriate advice and assistance to the requester submit a refined request. The Council is awaiting a response from the ICO on the remaining complaints.

Table 1. Number of FOI/EIR requests received

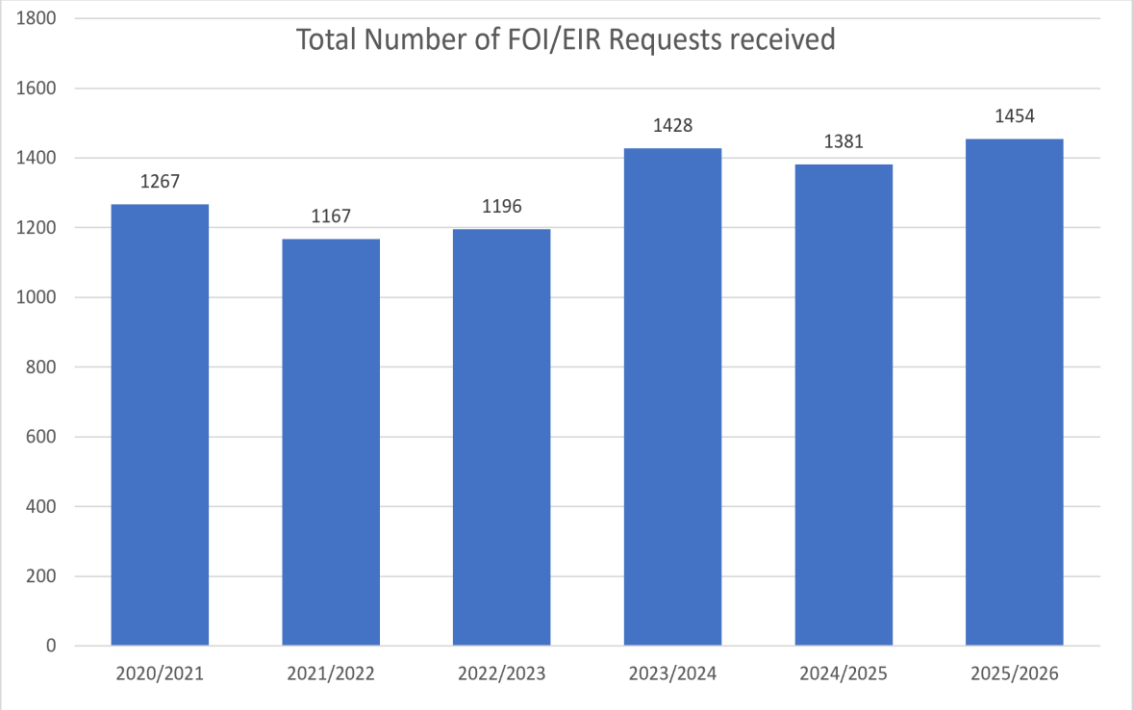
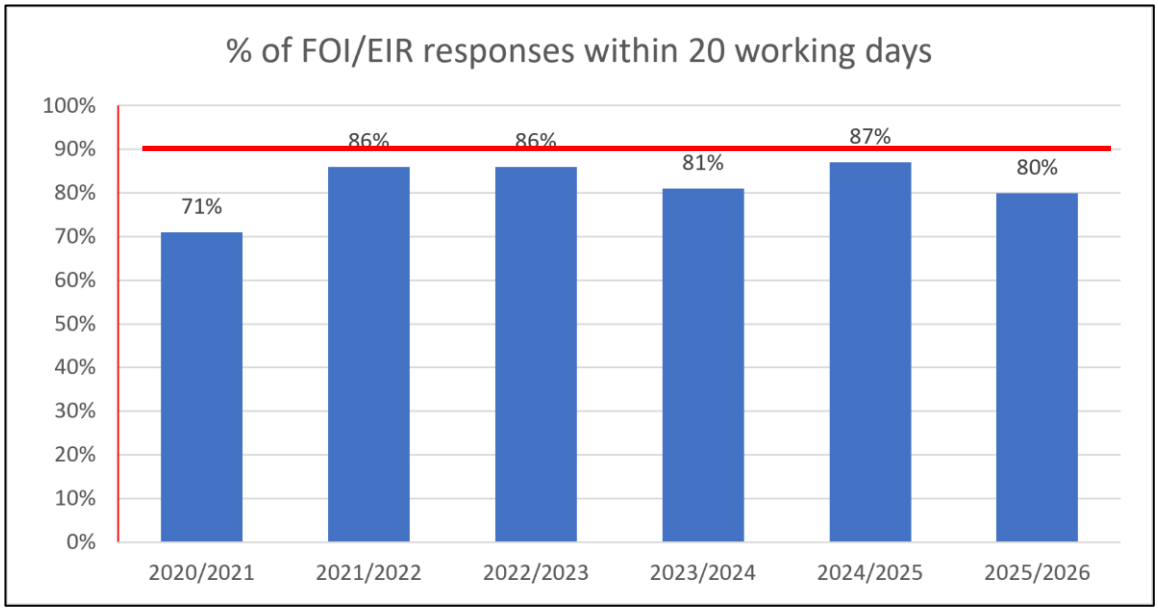


Table 2. Proportion of FOI/EIR requests completed within target time



2.2.5 370 valid Subject Access Requests (SARs) were received during 2025/26 which is a huge increase from 2024/25 (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 reduced to 67% in 2025/26, down from 71% the previous year.

2.2.6 The Council received 31 requests to carry out an internal review into a SAR application during 2025/26, up from 19 the previous year. The majority of these have now been closed to the satisfaction of the requester, but 5 remain live and the team are endeavouring to deal with these without reversion to the ICO.

2.2.7 To date, the Council has been contacted about one complaint made to the ICO in relation to Subject Access Requests during 2025/26, compared with three in the previous year. However, the Council is aware that the ICO is experiencing a significant increase in complaints and is consequently operating with a substantial backlog so this position may change. The one complaint concerning subject access rights has been closed by the ICO with no further recommendations.

Table 3. Number of SARs received

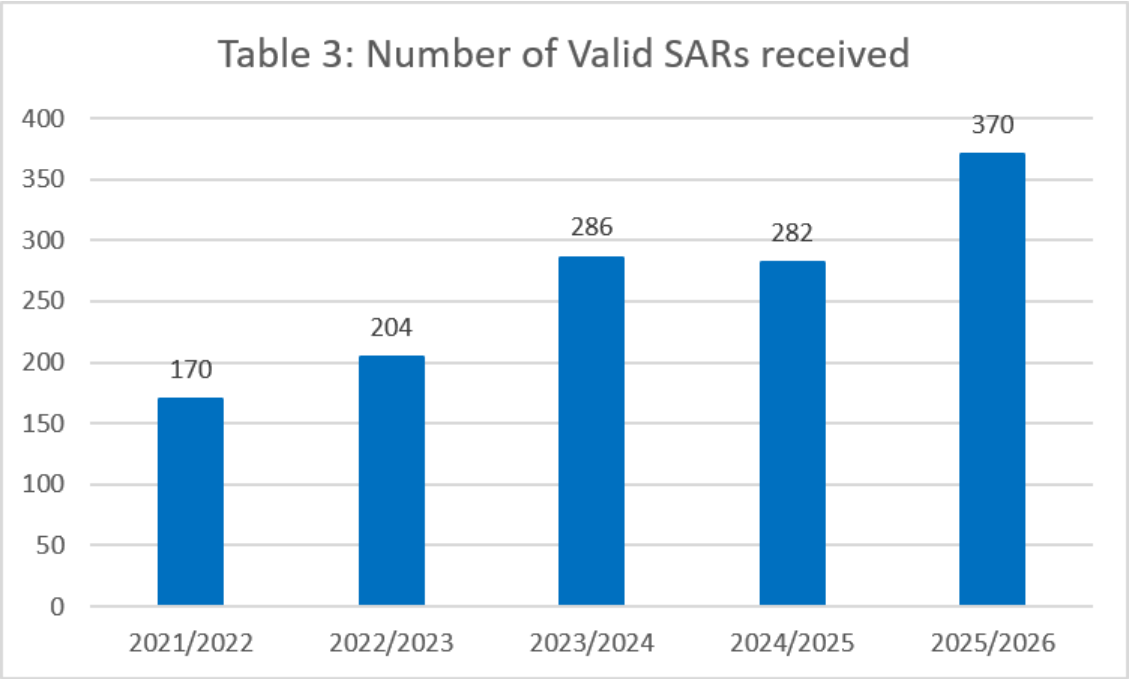
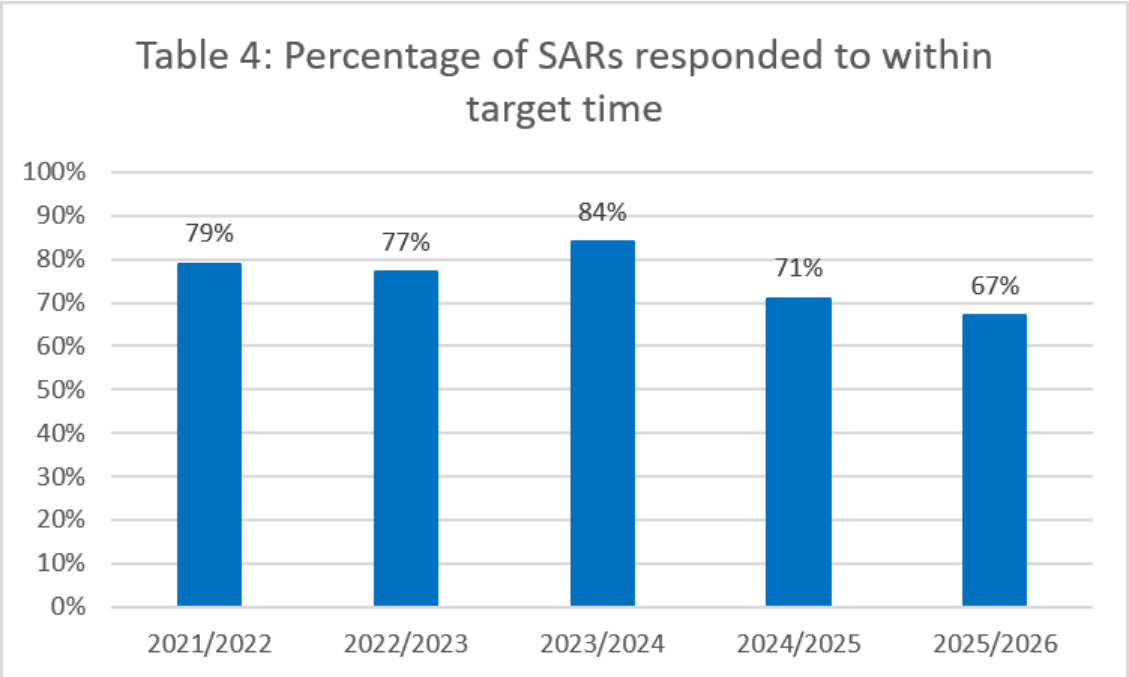


Table 4. Proportion of SARs responded to within target time



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. During the year, targeted campaigns were carried out to promote the importance of reporting incidents. When investigating data protection security incidents, the Data Protection Team routinely considers resultant training needs and provides advice and guidance as required. Communications continue to be provided to staff alerting them to the need to protect personal data and use it appropriately.

2.3.4 In 2025/26, 214 information security incidents were recorded by the Data Protection Team, compared with 168 in the previous year. Of these reports, 147 did not involve a breach of personal data as the incident was contained, for example where technical measures prevented access to data or information was returned or deleted. The majority of reports related to technical or procedural errors, followed by information disclosed in error, loss or theft of hardware, and unauthorised access. Technical and Procedural Breaches during 2025/26 included disclosure following the improper application of redactions, a confidential spreadsheet being attached to an email, emails being forwarded in error and letters being overwritten with original personal information left in.

2.3.5 The GDPR introduced requirements for personal data breaches that meet certain thresholds to be reported to the ICO. During 2025/26, 5 breaches were self-reported to the ICO by the Council.

2.3.6 There has been one complaint from a data subject following a data breach to the ICO. They have confirmed that they do not intend to take regulatory action and provided guidance on measures to help prevent similar incidents in future.

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. Other information and awareness raising is undertaken throughout the year in response to local and national issues. During 2025/26, the team delivered targeted training to Children's Services following a number of data breaches, to reinforce data protection responsibilities and support improvements in practice.

2.4.3 For 2025/26, the Council achieved a 95% completion rate for mandatory data protection training. Data protection training is also included within the Elected Member Training and Development Strategy. The Information Governance Manager delivered data protection training for elected Members on 7 and 9 July 2026, with further mop-up sessions planned for October 2026.

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 2025/26 reporting period, the Council met all the mandatory requirements and was assessed as having met standards and has achieved the necessary assurance.

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, Governance and Safer Communities

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?

(https://www.coventry.gov.uk/strategies-plans-policies/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 authors:
Adrian West
Head of Governance / Data Protection Officer

Gemma Harris
Information Governance Manager

Directorate:
Law, Governance and Safer Communities

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	Directorate	Date doc sent out	Date response received or approved
Contributors:				
Michelle Salmon	Governance Services Officer	Law, Governance and Safer Communities	03/09/26	04/09/26
Sue Gilbert	Information Governance Officer	Law, Governance and Safer Communities	03/09/26	07/09/26
Preeti Mistry	Information Governance Officer	Law, Governance and Safer Communities	03/09/26	07/09/26
Rebecca Newstead	Information Governance Officer	Law, Governance and Safer Communities	03/09/26	07/09/26
Names of approvers for submission: (officers and members)				
Cath Crosby	Lead Accountant, Financial Management	Finance and Resources	03/09/26	10/09/26
Syeda Ahmed	Regulatory Services Team Leader	Law, Governance and Safer Communities	03/09/26	07/09/26
Julie Newman	Director of Law, Governance and Safer Communities	-	03/09/26	10/09/26
Councillor G Duggins	Leader and Cabinet Member for Policy and Leadership	-	03/09/26	03/09/26

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