East Lothian Council

COMMITTEE: AUDIT AND GOVERNANCE COMMITTEE

MEETING DATE: 16 JUNE 2026

BY: DEPUTY CHIEF EXECUTIVE, RESOURCES & ECONOMY

REPORT TITLE: INFORMATION GOVERNANCE ANNUAL REPORT

REPORT STATUS: PUBLIC

1 PURPOSE OF REPORT

1.1 To report on the delivery and continuous improvement of East Lothian Council's ('the Council's) compliance with regulatory regimes relating to Data Protection, Information and Records Management, and the Regulation of Investigatory Powers during 2025.

2 RECOMMENDATIONS

Members are recommended to:

2.1 Note the contents of the report and, where appropriate, highlight areas for further action or consideration.

3 BACKGROUND

3.1 Information Governance covers a range of policies, procedures, tools and guidance used to support the Council in maintaining compliance with information legislation, ensuring that our information assets remain relevant and accessible over time, and empowering both the Council's employees and the citizens of East Lothian to derive the greatest possible benefits from the valuable public records in our custody.

3.2 A summary of the relevant legislation and key features is provided in Appendix 1 to this report.

3.3 Changes to legislation include the introduction of the Data Use and Access Act 2025, which supplements and clarifies existing legislation.

Data Protection

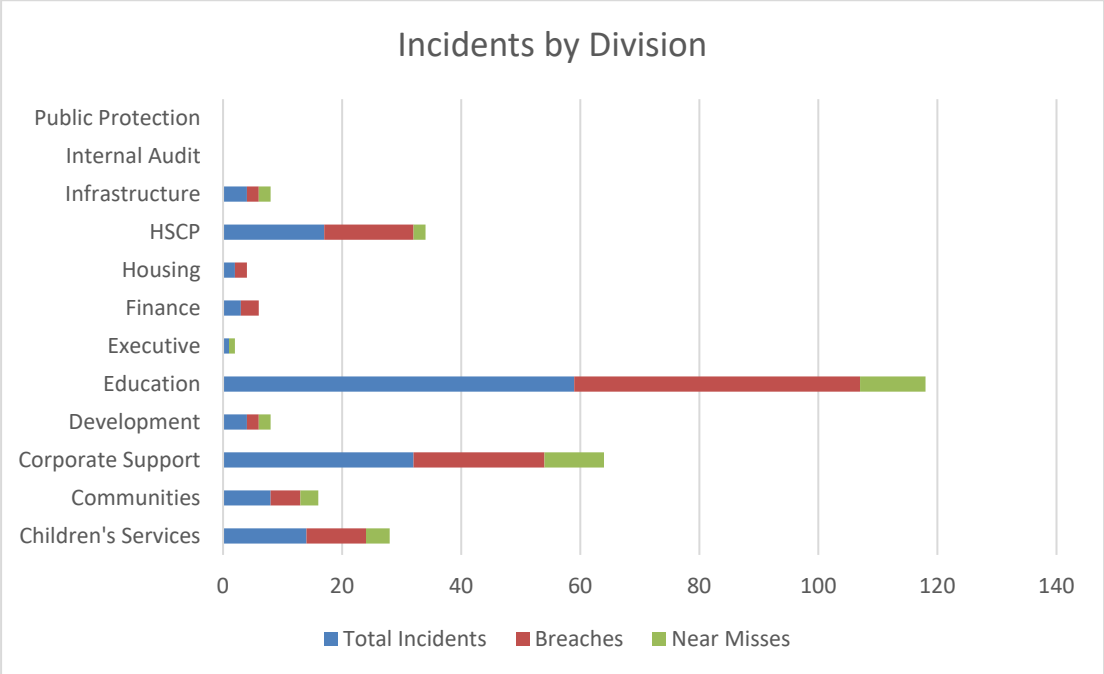
3.4 The protection of personal data in the UK is governed by the Data Protection Act 2018 ('DPA2018') and the UK General Data Protection Regulation ('UK GDPR'). In 2018, the Council implemented a raft of measures to support compliance and has continued to develop and enhance these measures year on year.

3.5 The Council's Information Governance staff continue to work with Procurement, IT and Legal Services to streamline the process for conducting Data Protection Impact Assessments (DPIAs) and the establishment of Data Sharing Agreements (DSAs) with contractors and data sharing partners.

Data Breaches

3.6 The Council's Data Breach Procedure requires all staff to report personal data breaches internally to the Council's Data Breach Team within 24 hours, to allow for a risk assessment and a decision to be taken whether to formally report to the national regulator, the Information Commissioner's Office ('ICO'). Where incidents meet the threshold of 'likely risk' to the rights of the data subject, by law the Council must report to the ICO within 72 hours; where incidents meet the threshold of 'high risk' to the data subject, the Council must also report the incident to the data subject(s) concerned.

3.7 Data breaches can present significant financial and reputational risks to the Council; the ICO has the power to levy significant fines and/or take enforcement action where significant or systemic failures are identified. Over the course of 2025, the Council recorded 109 Data Breaches and 35 Near Misses, resulting in a total of 144 incidents, a 47% increase compared with 2024. These incidents occurred across Council Divisions as follows:

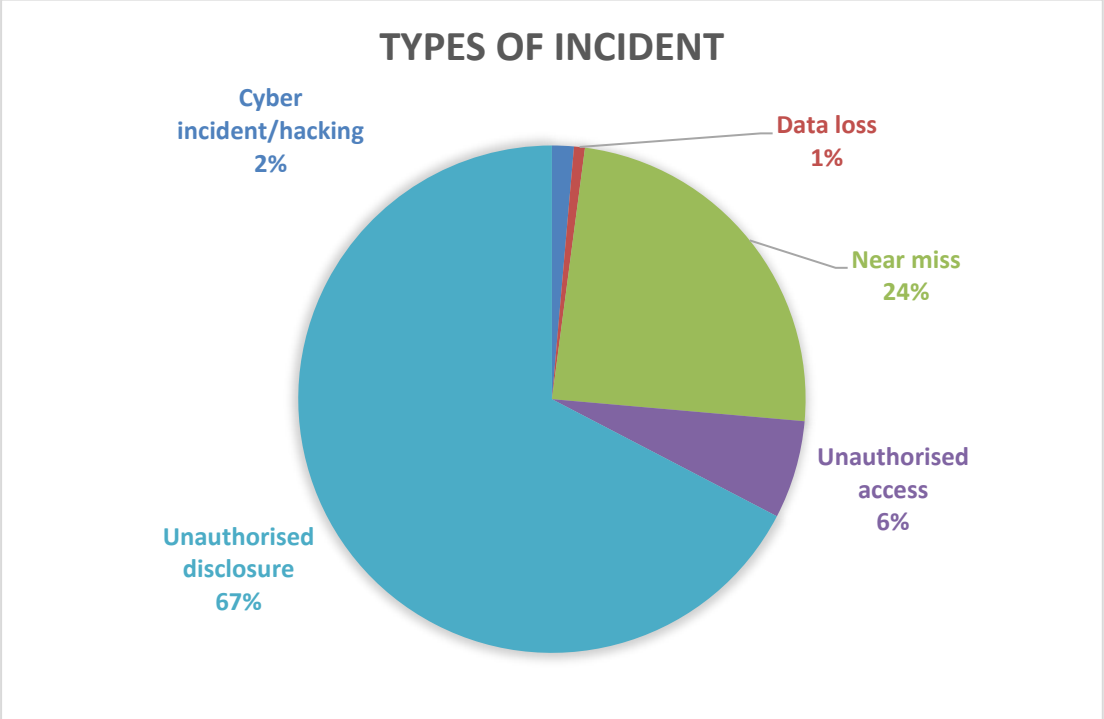


3.8 A total of eight incidents were reported to the Information Commissioner's Office – a 100% increase on breaches reported in 2024. In all eight cases, the ICO found that the Council had appropriate technical and organisational measures in place and took no further action.

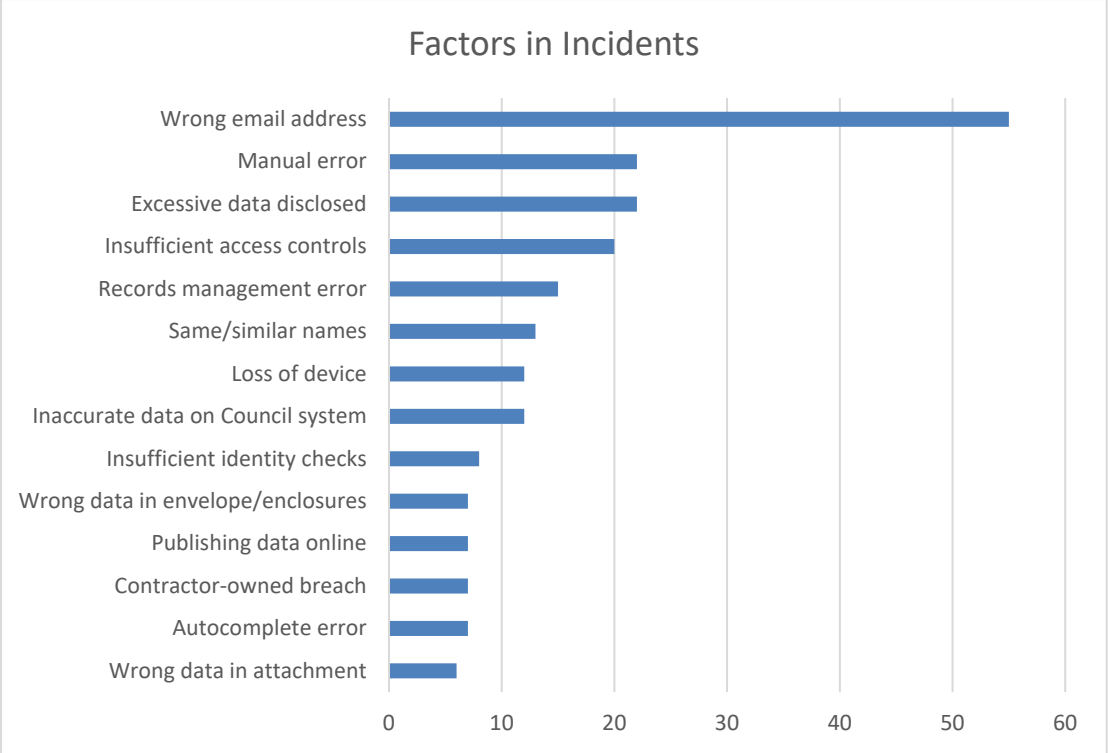
3.9 The most prevalent type of incident was unauthorised disclosure, i.e. the unnecessary or disproportionate sharing of Council-controlled personal data. There were also several incidents of unauthorised access, i.e. gaining or procuring access to Council systems without an authorised business purpose for doing so.

3.10 2025 has also seen a slight decrease in the number of cyberattacks reported by Suppliers involving Council-controlled data. Where appropriate, the Council continues to liaise actively with these Suppliers to ensure that all appropriate remedial action is taking place to reduce the impact of these incidents and the likelihood of recurrence in future. Where appropriate, the Council is seeking to change Supplier in cases where the balance of risk and business benefits no longer meets the Council's needs.

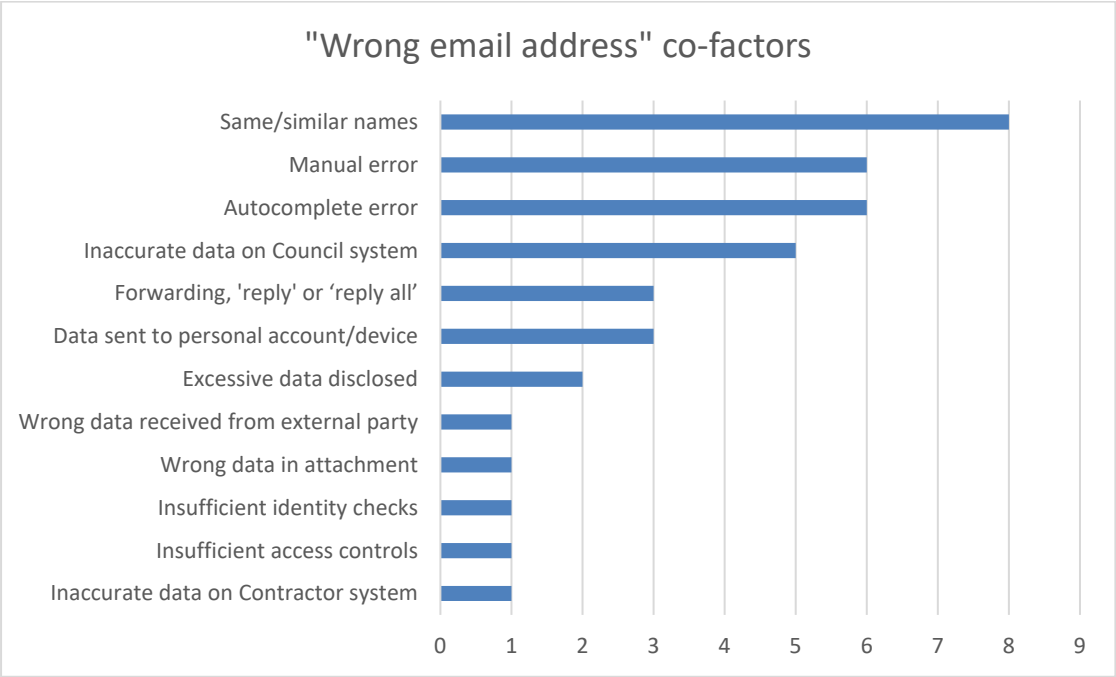
3.11 In addition to Data Breaches, the Information Governance team tracks Near Misses to gather additional data, identify trends and put appropriate preventative measures in place. The Council is not required by law to track Near Misses, but this provides a useful tool in understanding information management practices and where/how breaches might arise.



3.12 There are a number of trends evident in the factors and circumstances contributing to incidents (including both Data Breaches and Near Misses). The most frequently occurring factor by far remains the misdirection of email, which occurred in 55 instances.



3.13 The factors identified above might not occur in isolation, i.e. a single incident might involve multiple factors. For example, an incident might involve the use of a 'wrong email address' due to the individual 'using "to" or "cc" instead of "bcc", and so both are recorded as relevant factors to the incident. The chart below identifies the factors that most commonly appear alongside a 'wrong email address':



3.14 Regarding the eight breaches reported to the ICO, contributing factors included:

- Manual error
- Records management errors
- Excessive data disclosed
- Publishing data online
- Inaccurate data on Council systems
- Wrong data posted, sent home or included in envelopes
- Wrong email address

3.15 While the ICO did not find enforcement action to be necessary in relation to the eight reported incidents, they did make a number of recommendations for the Council to consider going forward, including:

- Continuing to review our processes and procedures when changing or adding personal data to systems, for example enacting a policy whereby staff do not work on more than one record simultaneously;
- Implementing double-checking processes when changing or adding usernames/identity information to accounts;
- Reviewing the contents and frequency of data protection training, including role-specific training;
- Maintaining awareness of data protection amongst staff via the use of routine reminders provided through staff emails/newsletters, staff intranet, team meetings, posters and screensavers;
- Conducting quality assessment checks at reasonable intervals;
- Ensuring staff have the time they need to double-check their work to prevent further breaches;
- Increasing awareness and reviewing our policies for handling the personal data of those at most risk of harm. This may involve additional training to relevant members of staff, systematic tools to mark and track those at most risk of harm and well circulated policies for handling their data with sensitivity.

3.16 Three incidents were considered to meet the statutory ‘high risk’ threshold requiring reporting to the Data Subject(s). These incidents primarily involved manual errors, but also included emails sent to the wrong email address on the basis of inaccurate data held on Council systems.

Trends, lessons learned and next actions

3.17 Every data incident is assessed on a case-by-case basis, and accordingly the Information Governance team makes recommendations to Services for future improvements to their information management practices. In some cases, additional technical measures can be put in place, for example putting labels in Active Directory that identify employees with the same or similar names by department. Many cases, however, and particularly those involving misdirected email, require careful manual checking by individual employees, relying on their professional knowledge and training to maintain compliance.

3.18 In 2024, the Council recorded 71 data breaches and 27 near misses, resulting in a total of 98 incidents reported over the year. This means that 2025 has seen a 47% increase in the number of incidents reported compared with 2024, and a 71.4% increase compared with 2023. While this increase could be due to an increase in reporting, the extent of this increase is unlikely to be due to reporting alone. Accordingly, a key priority for 2026 will be the expansion of training for all staff on data protection compliance, information security, and records management.

3.19 Overall, the profile of the types of incident, factors in incidents and distribution of incidents in Council Services has remained similar to that of 2024; in 2024 the most prevalent factor in incidents was the use of the wrong email address, with same/similar names and manual errors the primary co-factors. The re-introduction of the autocomplete feature within Outlook has also contributed to the rise in email breaches, and there has been a marked increase in breaches with records management errors as a contributing factor. Unauthorised disclosure continued to be the most frequent type of breach, with the greatest number of incidents continuing to occur in Education.

3.20 In 2025 we have seen a slight increase in email breaches where the use of “to” or “cc” instead of “bcc” has been a factor compared with 2024, when it was a target for awareness-raising by the Information Governance / IT teams.

3.21 In relation to incidents reported to the ICO, the ICO has consistently highlighted points of good practice by the Council in relation to our policies, procedures, staff training and incident response. Recognising this, we remain committed to continuous improvement in data protection compliance across the organisation.

2025 Actions Taken:
• Delivered a programme of training sessions across the Council on data breaches, DPIAs and records management • Continued development of MetaCompliance to enhance training and awareness • Undertook testing of data breach reporting functionality within MetaCompliance in preparation for wider rollout

• Supported services in the completion and review of DPIAs and strengthened related processes • Increased engagement with services to provide advice and support on data protection compliance • Developed guidance and supporting materials to improve understanding of data protection requirements • Promoted information governance awareness across the organisation • Initiated development of compliance monitoring and governance arrangements
2026 Planned Actions:
• Deliver a targeted Information Governance improvement programme across services, focusing on training, DPIAs and privacy compliance • Implement corporate data breach reporting via MetaCompliance to enhance oversight and learning • Strengthen DPIA processes, monitoring and reporting to embed privacy-by-design • Develop and implement an AI governance framework and policy aligned with Scottish Government initiatives, ensuring safe and ethical use • Introduce a structured compliance monitoring and assurance programme • Review and strengthen Data Sharing Agreements across the Council • Undertake a corporate review of privacy notices to improve transparency and consistency • Enhance management information and reporting to support governance oversight • Promote a culture of accountability and awareness across services

Records Management

3.22 The Public Records (Scotland) Act 2011 ('PRSA') requires public authorities to develop and maintain a Records Management Plan ('RMP') subject to approval by the Keeper of the Records of Scotland ('the Keeper'). East Lothian Council's first and current RMP was approved in 2015 on an 'improvement plan' basis, highlighting a number of areas for ongoing development and improvement. The Council has continued to engage constructively with the Keeper's Assessment Team via a process of voluntary annual review since 2015, apart from a brief hiatus over the period of the pandemic. The Keeper has now reduced the review interval from annual to bi-annual.

3.23 In 2025, the Council mobilised its contract with an external document management service provider and is currently engaged in transferring the contents of its paper records store to the provider's facility. This move brings significant improvements to both compliance and service levels for records storage and security, making records more accessible and our services more resilient.

3.24 The Information Governance team continues to contribute to the Microsoft 365 ('M365') implementation project, including the completion of a pilot

SharePoint site and digital document store for Legal Services. The Information Governance features of M365 are robust and will allow the automatic application of retention rules to individual records belonging to all Council Services as well as automatic version control and tracking. This is a key step in practically applying the Records Management Plan to the Council's digital records and will provide a significant improvement to compliance.

3.25 The Council's digital preservation programme has continued to progress, including the creation of a digital asset register and the introduction of essential checks and maintenance of our permanent digital collections. Work will continue to procure appropriate technical tools to ensure that our records remain accessible over time.

3.26 The Council's Records Management Plan is modelled after the Keeper's Model Plan, which at the time of creation included 14 Elements (now 15 for current submissions).

2025 Actions Taken:
• Review of the corporate retention schedule continued on a service-by-service basis; • Information Officers continued to feed in to the national group addressing model retention schedules for Scottish Local Authorities; • Indexing and transfer of paper Planning files by document management Supplier; • Digital Asset Register and Digital Preservation Audit Dashboard created for digital items in custody of the Council Archives; • Records retention labelling, security classification and other key governance features went under testing in Microsoft Purview, to support the wider implementation of SharePoint and Microsoft 365; • Records management training module published to Council Intranet.
2026 Planned Actions:
• Progress the digital preservation programme, including options for a digital repository; • Complete and sign off Information Strategy to support the Council's Digital Strategy; • Complete transfer of the paper records store to the contracted Supplier; • Continue to support M365 implementation; • Collaborate with the Team Manager-Information and Feedback to promote Records Management training and awareness; • Continue to develop tools to assist managers across Services to monitor Supplier compliance with records management requirements in line with national guidance.

<u>Covert Surveillance</u>

3.27 The Regulation of Investigatory Powers (Scotland) Act 2000 ('RIPSA') was enacted to provide a statutory framework for the operation of covert surveillance investigative techniques by public authorities. This framework gives public authorities powers to undertake necessary and proportionate

surveillance while respecting the individual's 'right to respect for private and family life' under the Human Rights Act 1998 ('HRA').

3.28 In order to carry out surveillance under RIPSA, Council officers must follow a prescribed statutory process, according to statutory roles and responsibilities. In order to undertake an investigation under RIPSA, the Investigating Officer must submit an application to a senior Authorising Officer, who must consider and document the decision to proceed. This process exists primarily to ensure that risks have been considered appropriately that effective mitigations are put in place, that the investigation is fully documented to appropriate standards, and that the investigation is monitored and reviewed over time.

3.29 East Lothian Council has to-date made very limited use of its RIPSA powers, and there were no applications made in 2025.

3.30 At the end of 2024, the Council was advised that an inspection by the Investigatory Powers Commissioner's Office ('IPCO') would not be required in 2025, due to the Council's appropriate level of compliance. The next inspection by the IPCO will be in 2028.

2025 Actions Taken
• Documentation updated.
2026 Planned Actions
• Training and awareness resources to continue to be developed and publicised;

4 POLICY IMPLICATIONS

4.1 This report supports and evidences compliance with the following Council Policies:

- Data Protection Policy
- Information and Records Management Policy
- Records Management Plan
- RIPSA Policy

5 RESOURCE AND OTHER IMPLICATIONS

5.1 Finance: None

5.2 Human Resources: None

5.3 Other (e.g. Legal/IT): This report supports and evidences the Council's compliance with information legislation, including the Data Protection Act 2018 / UK GDPR, the Data Use and Access Act 2025, the Public Records (Scotland) Act 2011 and the Regulation of Investigatory Powers (Scotland) Act 2000.

5.4 Risk: The occurrence of data breaches carries the risk of reputational damage, financial penalty and/or other enforcement action against the Council by the Information Commissioner's Office (ICO). Failure to adhere to the Council's Records Management Plan and RIPSA Policy also carry the risk of enforcement action by the relevant regulators. These risks are regularly reported and managed via the Council's corporate and service-level risk registers, as well as the cross-operational Linking Risks group.

6 INTEGRATED IMPACT ASSESSMENT

6.1 ***Select the statement that is appropriate to your report by placing an 'X' in the relevant box.***

An Integrated Impact Assessment screening process has been undertaken, and the subject of this report does not affect the wellbeing of the community or have a significant impact on: equality and human rights; tackling socio-economic disadvantages and poverty; climate change, the environment and sustainability; the Council's role as a corporate parent; or the storage/collection of personal data. [X]

or

The subject of this report has been through the Integrated Impact Assessment process and impacts have been identified as follows: [ ]

Subject	Impacts identified (Yes, No or N/A)
Equality and human rights	
Socio-economic disadvantage/poverty	
Climate change, the environment and sustainability	
Corporate parenting and care-experienced young people	
Storage/collection of personal data	
Other	

The Integrated Impact Assessment relating to this report has been published and can be accessed via the Council's website:

https://www.eastlothian.gov.uk/info/210602/equality_and_diversity/12014/integrated_impact_assessments

7 APPENDICES

7.1 Appendix 1 – Legislation Key Features

8 BACKGROUND PAPERS

8.1 None

9 AUTHOR AND APPROVAL DETAILS

Report Author(s)

Name	**Zarya Rathé and Nikki Brennan**
Designation	**Team Manager-Information and Records Management; Team Manager-Information and Feedback**
Tel/Email	**zrathe@eastlothian.gov.uk; 01620 827989** **nbrennan@eastlothian.gov.uk; 01620 827195**
Date	**05/06/2026**

Head of Service Approval

Name	**Sarah Fortune**
Designation	**Depute Chief Executive Resources and Economy**
Confirmation that IIA and other relevant checks (e.g. finance/legal) have been completed	**Confirmed**
Approval Date	**09/06/2026**

APPENDIX 1

Legislation	Key Features
Data Protection Act 2018 / UK GDPR	• Governs the protection of **personal data**; • Mandatory recording and reporting of **personal data breaches**. Any breach meeting the 'likely risk' threshold must be reported to the UK Information Commissioner's Office ('ICO') within 72 hours. Any breach meeting the 'high risk' threshold must be reported to the data subject(s). • A 'personal data breach' is defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.'
Data Use and Access Act 2025	• **Amends** existing UK data protection legislation, including the UK GDPR, Data Protection Act 2018 and Privacy and Electronic Communications Regulations; • Introduces a range of **reforms** to support more **flexible and efficient use of data**, while maintaining safeguards for individuals' rights; • Includes updates to areas such as automated decision-making, subject access requests, scientific research provisions and international data transfers; • Introduces a new statutory right for individuals to complain directly to organisations about the handling of their personal data; • Requires organisations to implement a **formal data protection complaints process**, including clear routes for complaints, timely acknowledgement and response, and communication of outcomes; • Forms part of a wider programme of reform to enable responsible data sharing and innovation across the UK economy.
Public Records (Scotland) Act 2011	• Governs the management of **public records**;

	• All named authorities must create a 15-point **Records Management Plan** in line with the Model Plan created by the Keeper of the Records of Scotland ('the Keeper'); • Authorities can undergo **optional review** of their Records Management Plans by the Keeper's Assessment Team on an annual basis, called the 'Progress Update Review Mechanism' ('PUR'). This is not mandatory, but active engagement provides greater assurances regarding the authority's compliance.
Regulation of Investigatory Powers (Scotland) Act 2000	• Governs the use of **covert surveillance**; • Provides a framework for public officers to undertake **necessary and proportionate surveillance** while maintaining compliance with 'the right to respect for private and family life' under the Human Rights Act 1998; • RIPSA investigations undergo a rigorous **process of authorisation and review** with frequent oversight by qualified Senior Officers within the Council; • Only applies to '**core functions**,' i.e. the specific public functions undertaken by a particular authority. It does not apply to 'ordinary functions' such as employment/Human Resources which are undertaken by all authorities.