East Lothian Council

REPORT TO: **AUDIT AND GOVERNANCE COMMITTEE**

MEETING DATE: **17 JUNE 2025**

BY: **EXECUTIVE DIRECTOR-COUNCIL RESOURCES**

SUBJECT: **INFORMATION GOVERNANCE ANNUAL REPORT**

---

1 PURPOSE

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 2024.

2 RECOMMENDATIONS

2.1 To 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.

Data Protection

3.3 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 new measures to support compliance; these measures were subject to their first assessment by the Council's Internal Auditors in November 2022.

3.4 The audit found reasonable assurance overall, with multiple points of good practice noted as well as a number of recommendations made for further improvements.

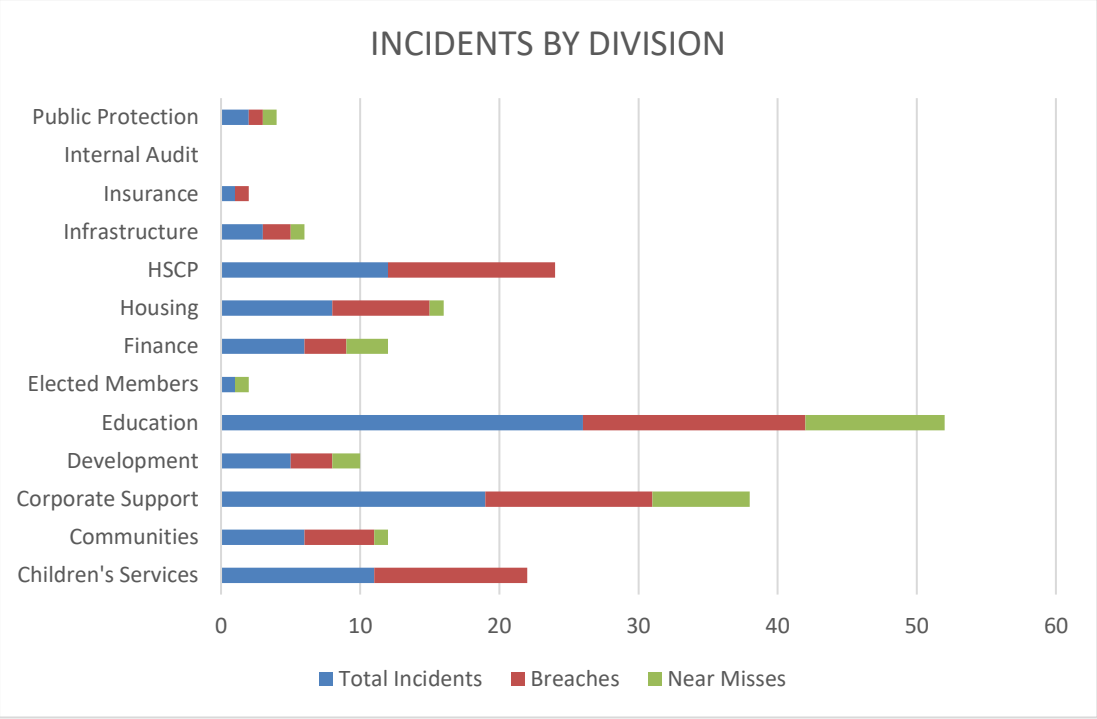
3.5 The audit identified five recommendations overall, of which four are currently complete and one is partially complete. The outstanding action relates to the timely completion of Data Protection Impact Assessments ('DPIAs') and Data

Sharing Agreements ('DSAs'). With the recruitment of a new Team Leader the backlog of DPIAs and DSAs has considerably reduced. Work is ongoing to further reduce the backlog of approvals and improve processing times for new DPIAs.

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 2024, the Council recorded 71 Data Breaches and 27 Near Misses, resulting in a total of 98 incidents. These incidents occurred across Council Divisions as follows:

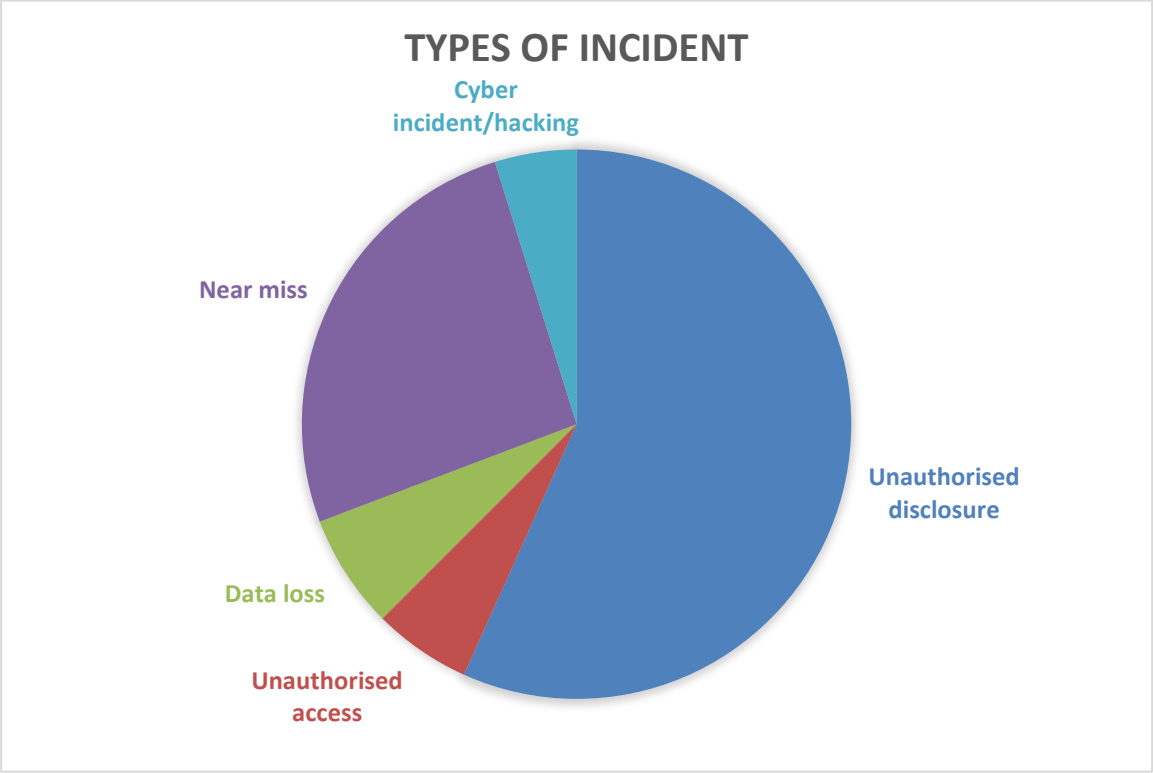


3.8 A total of four incidents were considered to meet the 'likely risk' threshold for reporting to the Information Commissioner's Office. In all four cases, the ICO found that the Council had appropriate technical and organisational measures in place, and took no further action.

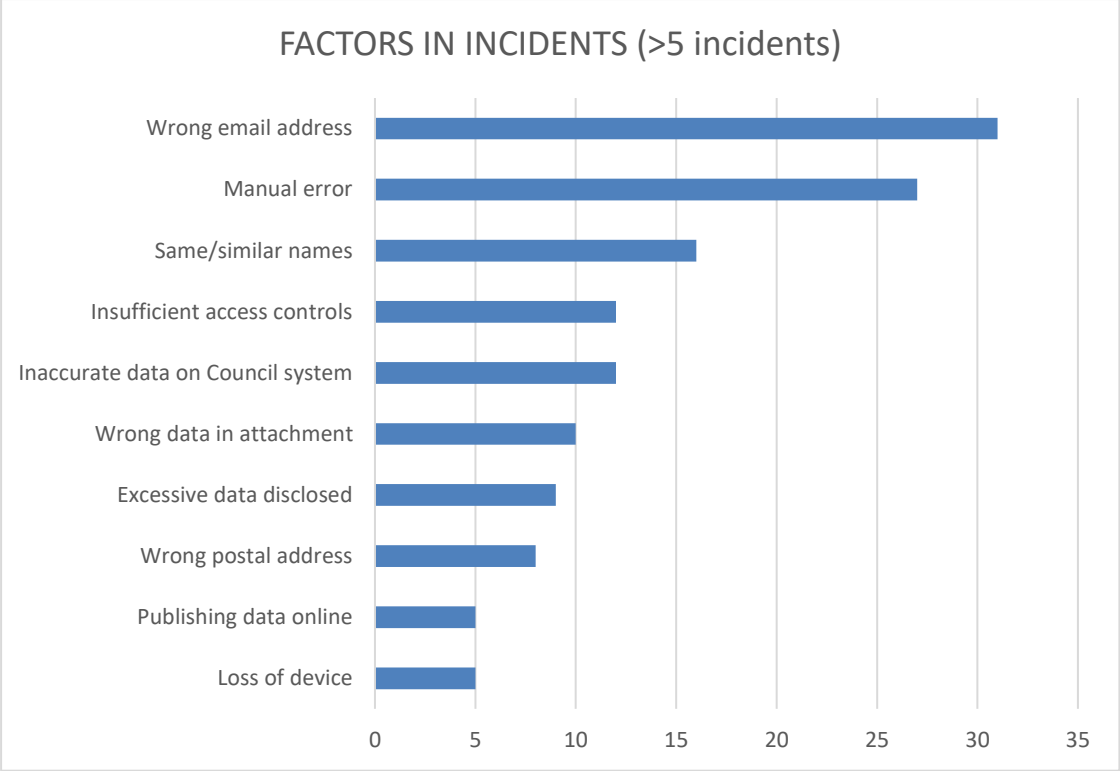
3.9 The most prevalent type of incident was unauthorised disclosure, i.e. the unnecessary or disproportionate sharing of Council-controlled personal data. There were also several incidents of unauthorised access, i.e. gaining or procuring access to Council systems without an authorised business purpose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

3.10 2024 has also seen an increase 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.

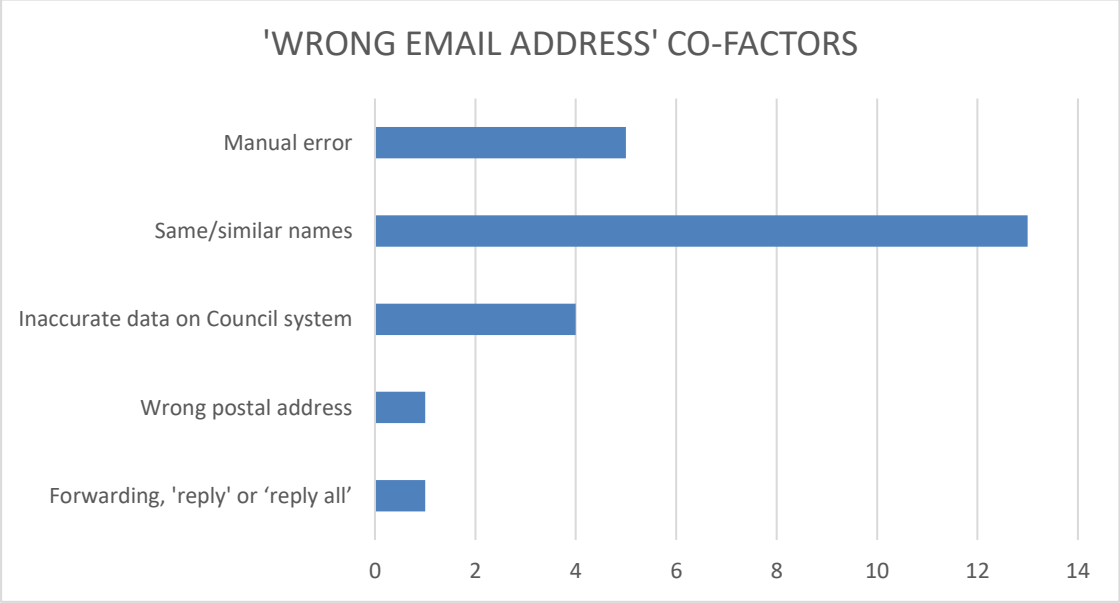
3.11 In addition to Data Breaches, the Information Governance team tracks Near Misses to gather additional data, identify trends and put appropriate preventative measures in place. The Council is not required by law to track Near Misses, but this provides a useful tool in understanding information management 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 31 instances, although this represents a decrease from 45 instances in 2023.



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 four breaches reported to the ICO, contributing factors included:

- Manual error
- Inaccurate data on Council systems
- Loss of device / insufficient access controls (laptop stolen from car)

- Wrong data received from external organisations
- Redaction errors
- Publication of data online

3.15 While the ICO did not find enforcement action to be necessary in relation to the four 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 No incidents were considered to meet the statutory 'high risk' threshold requiring reporting to the Data Subject(s).

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 2023, the Council recorded 62 data breaches and 22 near misses, resulting in a total of 84 incidents reported over the year. This means that 2024 has seen a 16.7% increase in the number of incidents reported compared with 2023, and a 25.6% increase compared with 2022. It is important to note that while this increase could be due to an increase in the number of incidents that occurred, it is also possible that this is due to an increase in reporting.

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 2023; in 2023 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. Unauthorised disclosure was likewise the most frequent type of breach, with the greatest number of incidents occurring in Education.

3.20 In 2024 we have seen a drop in email breaches where the use of "to" or "cc" instead of "bcc" has been a factor, which has been a target for awareness-raising by the Information Governance / IT teams over 2024.

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. The Council's Internal Auditors have also found that we continue to have effective risk control measures in place. Recognising this, we remain committed to continuous improvement in data protection compliance across the organisation.

2022 Internal Audit Recommendations:
• Seek to ensure that relevant policies and procedures are reviewed on a regular basis; • Ensure that Data Sharing Agreements are put in place on a timely basis; • Ensure that appropriate progress is made in development of the Information Asset Register; • Ensure that timescales for planned risk control measures are realistic and implemented on a timely basis; • Roll out Communications Plan across the Council to reinforce the importance of Data Protection compliance.
2024 Actions Taken:
• Series of support sessions held for Head Teachers in conjunction with Legal Services; • Continued development of training via the compliance platform MetaCompliance, including a practice email phishing exercise; • Team Leader-Information Governance has delivered (and will continue to deliver) regular training on data protection, with an initial focus on DPIA completion; • DPIA 'triage' process introduced to improve submissions and prioritise assessment in line with Procurement priorities; • One Information Asset Register workshop conducted. In lieu of additional workshops, work is ongoing to replace the Register, in whole or in part, with features in Microsoft Sharepoint; • Data Breach reporting now set up within MetaCompliance and undergoing testing before wider roll-out to Services; • Regular meetings have been held (and will continue) between Information Governance, IT, Procurement and Business Transformation to continuously improve procurement processes and guidance for staff. This has included regular communication with Procurement to identify high-priority procurements and adjust Information Governance/IT priorities accordingly; • DSA and DPIA backlog reduced; all contracts using the Council's Standard Terms and Conditions now include a Data Protection Schedule as standard.

2025 Planned Actions:
• Supplement e-learning with face-to-face training sessions and recorded sessions; • Continue to develop and improve training and awareness through compliance software MetaCompliance; • Implement compliance features within Microsoft Sharepoint and Microsoft Purview; • Undertake regular reporting to senior managers on data breaches, security incidents and trends; • Development of an Information Strategy to underpin and support the Digital Strategy.

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. Since the last Information Governance Annual Report, the Keeper has reduced the review interval from annual to bi-annual.

3.23 A procurement mini-competition has recently closed to identify a best value Supplier for all storage, retrieval and destruction services for paper records. Following evaluation and selection of a Preferred Supplier, the contents of the Dunbar Road paper records store (c.8000 boxes) will be emptied and transferred to the chosen Supplier. This will introduce significant service improvements through flexible and responsive retrievals services, secure transactions and effective environmental controls.

3.24 The Information Governance team continues to contribute to the Microsoft 365 ('M365') implementation project. The team is currently supporting 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 Due to a combination of maternity leave and pressures on the Council's statutory information request-handling processes in 2024, a number of planned actions for records management from 2024 will carry forward into 2025. This includes progression of the Council's digital preservation programme, which has paused over 2024. This is expected to be re-instated in the second quarter of 2025-26.

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).

2022 Internal Audit Recommendations:
• Review guidance on Council Intranet; • Continue to develop the Information Strategy; • Complete record audits of Council offices in line with the Asset Review project; • Ensure that records retention rules are applied to digital records; • Continue to develop Information Asset Register, including as a tool to support the regular review/destruction of records; • Progress actions to address the long term preservation of digital records; • Ensure that a complete and accurate representation of changes to records' content and location is captured in relation to both paper and digital records ('audit trail'); • Review staff training requirements and ensure these remain up to date;
2024 Actions Taken:
• Corporate retention schedule reviewed and updated on a monthly basis. Legal Services schedule modified to conform to a more streamlined set of retention rules, which will be applied to other Services in 2025; • Information Officers continue to feed in to the national group addressing model retention schedules for Scottish Local Authorities; • Digital Preservation Policy approved; • Mini-competition for a Document Management Supplier (paper records storage) advertised, with evaluation currently in progress; • Records Management provisions designed for standard Supplier Scorecard;
2025 Planned Actions:
• Re-instate digital preservation programme, including options for a digital repository; • Complete and sign off Information Strategy; • Complete procurement for Document Management Supplier and commence transfer of records; • Continue to support M365 implementation; • Develop Records Management training and awareness; • Identify a new solution for disposal of confidential waste in collaboration with corporate Council projects; • Develop tools to assist contract managers across Services to monitor Supplier compliance with records management requirements in line with national guidance.

Covert Surveillance

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 2024.

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.

2023 Recommendations
• RIPSA Gatekeeper (Team Manager-Information Governance) to feed back to Investigating Officers via review of Application Forms prior to authorisation; • Business Classification Scheme / Retention Schedule to be updated to include RIPSA material; • E-learning module to be developed; • Service Manager-Governance to undertake external training.
2024 Actions Taken
• Documentation updated to reflect changes in staffing.
2025 Planned Actions
• Training and awareness resources to be developed and publicised; • Training sessions for specific Services to be held; • Service Manager-Governance to undertake re-scheduled training.

4 INTEGRATED IMPACT ASSESSMENT

4.1 The subject of this report does not affect the wellbeing of the community or have a significant impact on equality, the environment or economy.

5 RESOURCE IMPLICATIONS

5.1 Financial – there are no financial implications for this report.

5.2 Personnel - there are no personnel implications for this report.

5.3 Other – there are no other resource implications for this report.

6 BACKGROUND PAPERS

6.1 There are no background papers.

East Lothian Council

AUTHOR'S NAME	Zarya Rathé
DESIGNATION	Team Manager-Information Governance
CONTACT INFO	zrathe@eastlothian.gov.uk; 01620 827989
DATE	04/06/2025

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.'
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.