REPORT TO:	**AUDIT AND GOVERNANCE COMMITTEE**
MEETING DATE:	**26 MARCH 2024**
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 2023.

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. The Audit Report acknowledged that staffing challenges within the Information Governance team at the time contributed to risks, which were regularly highlighted in the Corporate Support and Corporate Risk Registers.

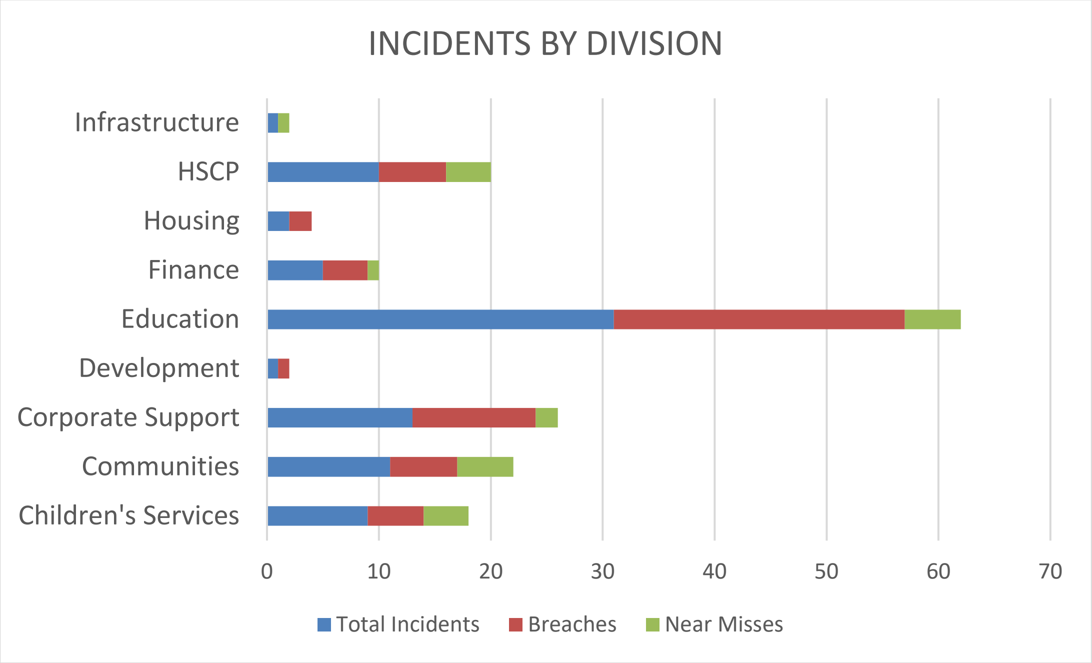
3.5 A new Team Leader-Information Governance post was created and recruited in August 2023. The capacity created by this additional post has been, and will continue to be, a key factor in making continuous improvements to the Council's compliance across Services going forward.

3.6 The audit identified five recommendations overall, of which four are currently complete and one is partially complete; these are also addressed by the Council's Internal Audit Service in their March 2024 report to the Audit and Governance Committee. The outstanding action relates to the timely completion of Data Protection Impact Assessments ('DPIAs') and Data Sharing Agreements ('DSAs'). With the recruitment of the new Team Lead the backlog of DPIAs and DSAs has considerably reduced, with a standard turnaround of 6 months reduced to 8 weeks. Work is ongoing to further reduce the backlog of approvals.

Data Breaches

3.7 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.

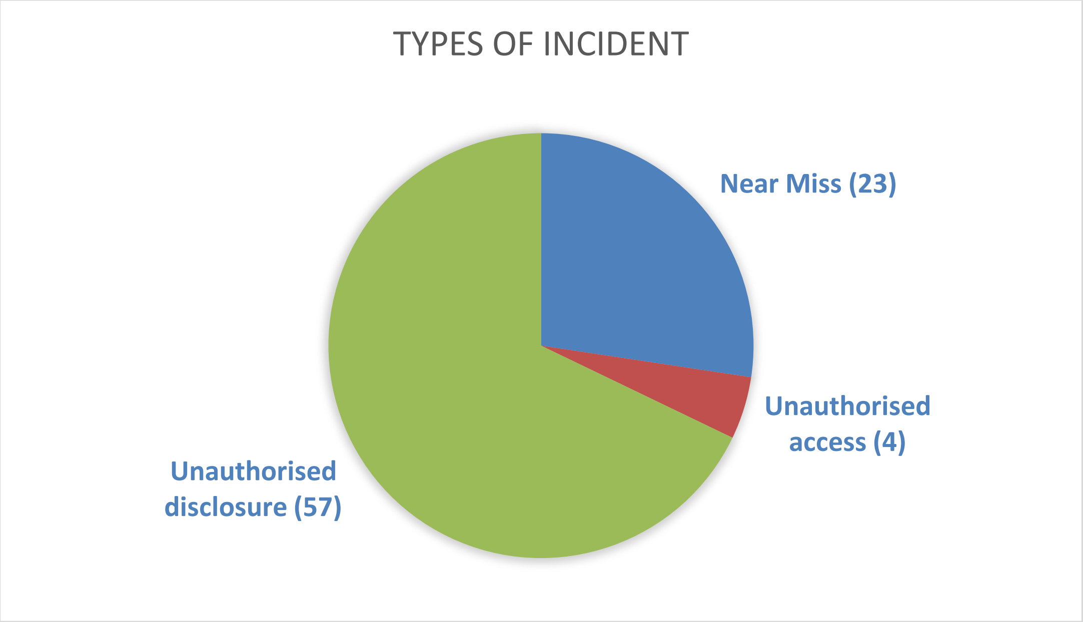
3.8 Data breaches can present significant financial and reputational risks to the Council; the ICO has the power to levy significant fines and/or take enforcement action where significant or systemic failures are identified. Over the course of 2023, the Council recorded **62** Data Breaches and **22** Near Misses, resulting in a total of **84** incidents. These incidents occurred across Council Divisions as follows:



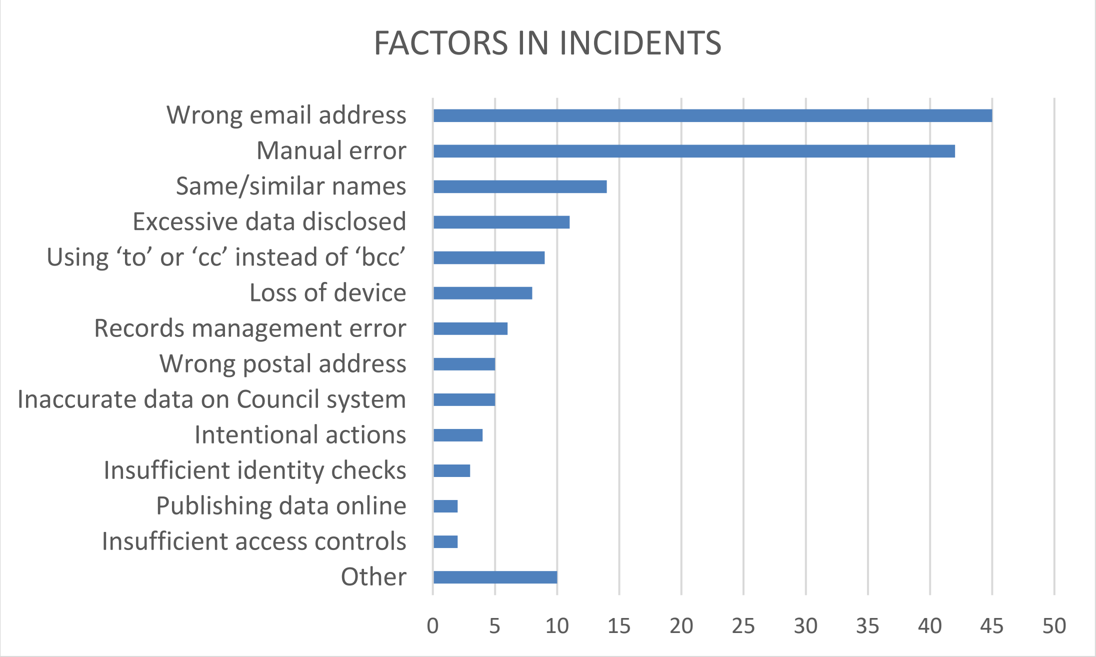
3.9 A total of **three** incidents were considered to meet the ‘likely risk’ threshold for reporting to the Information Commissioner’s Office. In all three cases, the ICO found that the Council had appropriate technical and organisational measures in place, and took no further action.

3.10 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.

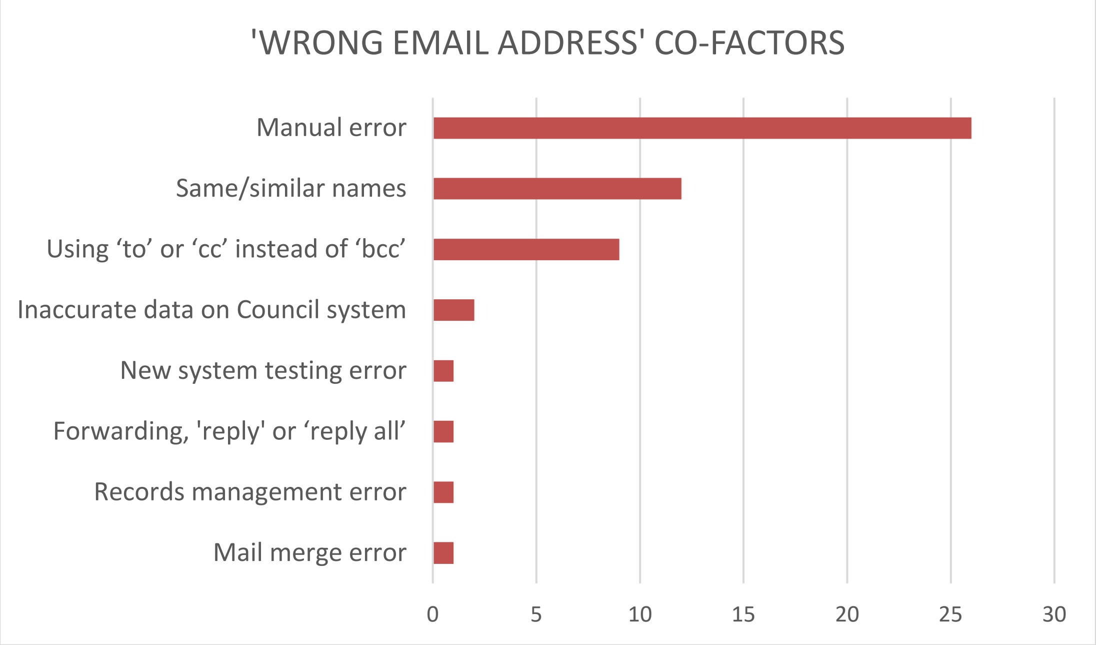
3.11 In addition to Data Breaches, the Information Governance team tracks Near Misses to gather additional data, identify trends and put appropriate preventative measures in place. The Council is not required by law to track Near Misses, but this provides a useful tool in understanding information management 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 is the misdirection of email, which occurred in **45** 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 three breaches reported to the ICO, contributing factors included:

- Wrong email address
- Using ‘to’ or ‘cc’ instead of ‘bcc’
- Manual error
- Same/similar names
- Insufficient identity checks

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

- Introduction of email safeguards such as default email delays, which can prevent incorrect emails from being sent, and secure email services, which can prevent a misdirected email from being opened entirely;
- Ensuring staff have the time they need to double-check their work to prevent further breaches.

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 2022, the Council recorded 53 data breaches and 24 near misses, resulting in a total of 78 incidents reported over the year. This means that 2023 has seen a 7.7% increase in the number of incidents reported. 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 simply 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 2022; in 2022 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 access was likewise the most frequent type of breach, with the greatest number of incidents occurring in Education.

3.20 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 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.
2023 Actions Taken:
• Additional Team Lead-Information Governance post created, with post-holder in place from August 2023; • Policies and Procedures updated to reflect current positions; • Standard waiting period for reviewing Data Protection Impact Assessments and Data Sharing Agreements reduced from 6 months to 8 weeks; • Information Asset Register workshops held in line with completion schedule, with Information Asset Owners and Administrators identified; • Data Protection risk control measures implemented in line with Corporate and Corporate Support risk registers; • Training and awareness campaign currently being launched via new software MetaCompliance integrated with Microsoft Teams, including training videos, assessment questionnaires, blog posts and policy documents. The first campaign event includes a phishing exercise to raise awareness regarding malicious emails; • Team Leader working closely with Education to develop a list of core approved applications for use in Schools and to identify gaps in data protection knowledge/training; • New and streamlined review/authorisation procedures have been implemented for Data Sharing Agreements (‘DSAs’) and Data Protection Impact Assessments (‘DPIAs’).
2024 Planned Actions:
• Series of support sessions for Head Teachers to be held in conjunction with Legal Services; • Development of ‘one stop shop’ for staff guidance, tools and training via MetaCompliance; • Information Asset Register workshops to be conducted quarterly, including identification of Information Asset Owners and Administrators; • Continue to explore technical options such as email delays and secure email services to reduce the risk of data incidents; • Complete development of a ‘Data Breach Dashboard’ to support high-level monitoring and reporting of data incidents to senior managers on a regular basis.

Records Management

3.21 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.

3.22 A procurement exercise remains in progress to identify a best value Supplier for all storage, retrieval and destruction services for paper records, and then 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.

3.23 The Information Governance team continues to contribute to the Microsoft 365 (‘M365’) implementation project team. 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.

3.24 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 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;
2023 Actions Taken:
• Council Intranet guidance reviewed and updated; • Office record audits completed, with Information Governance input into Asset Review project team meetings; • Corporate Council Retention Schedule reviewed and updated on a monthly basis in line with feedback from Services;

- ELC Information Governance staff regularly sit on the national working group responsible for developing the Scottish Local Authority standards for records retention;
- M365 implementation progressing, with Information Governance included in M365 Champions network and Project Team;
- Information Asset Register progressing in line with annual goals;
- Survey and register of digital assets for permanent preservation created;
- Digital Preservation Policy drafted and under final review;
- Options appraisal currently being developed for a digital repository solution for records of enduring business and historical value;
- Audit trail improved in relation to paper records transferred to off-site Supplier and digital records in the M365 environment;
- New provisions for records management and compliance with the Public Records (Scotland) Act 2011 have been added to the Council's Standard Terms and Conditions, tender documentation and Data Sharing Agreements.

2024 Planned Actions:

- Complete and sign off Information Strategy;
- Complete procurement for Document Management Supplier;
- Continue to support M365 implementation;
- Develop Records Management training and awareness via MetaCompliance 'one stop shop';
- Develop register of digital records for permanent preservation;
- Identify a digital preservation repository/solution for records of enduring value;
- 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.

<u>Covert Surveillance</u>

3.25 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').

3.26 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.

3.27 East Lothian Council has to-date made very limited use of its RIPSA powers, and there were no applications made in 2023.

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.
2023 Actions Taken
• RIPSA records included in corporate BCS / Retention Schedule.
2024 Planned Actions
• Training and awareness resources to be developed via MetaCompliance ‘one stop shop’; • 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 East Lothian Council Data Protection Audit Report (November 2022)

AUTHOR’S NAME	Zarya Rathé
DESIGNATION	Team Manager-Information Governance
CONTACT INFO	zrathe@eastlothian.gov.uk; 01620 827989
DATE	14/03/2024

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.