

REPORT TO: AUDIT AND GOVERNANCE COMMITTEE

MEETING DATE: 14 FEBRUARY 2023

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 over 2022.

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 have contributed to risks, which are regularly highlighted in the Corporate Support and Corporate Risk Registers. In

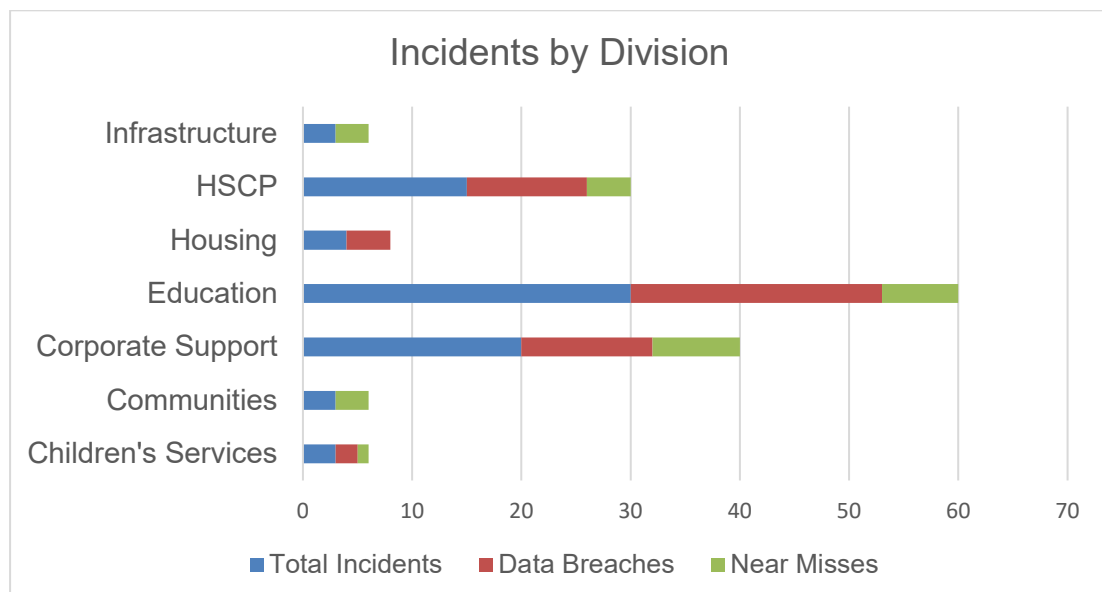
particular, a backlog of approvals for Data Sharing Agreements and Data Protection Impact Assessments has developed due to capacity challenges within the Information Governance team; likewise the population of the corporate Information Asset Register has made slow progress.

- 3.5 A summary of the audit's findings is presented in paragraph 3.17 under 'Lessons Learned' below, alongside feedback from the Information Commissioner's Office, actions taken and planned future measures.
- 3.6 The Information Governance team has recently created an additional Information Officer post, which was filled in early December 2022. The creation of a new Team Lead-Information Governance post is currently in progress and nearing completion. These additional posts will be a key factor in making continuous improvements to the Council's compliance across Services going forward.

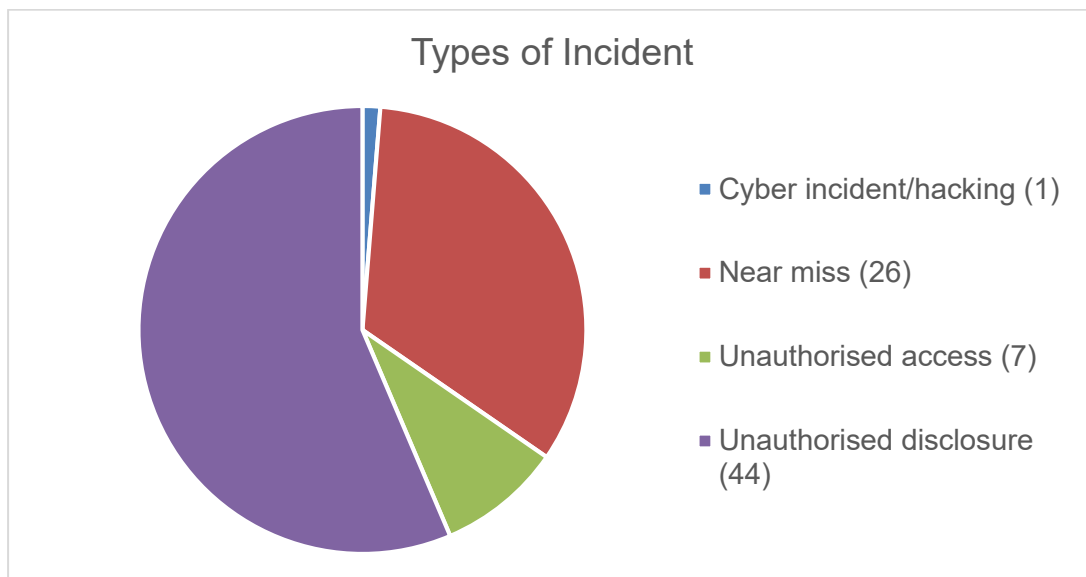
Data Breaches

- 3.7 The Council's current Data Breach Procedure was introduced in 2018. This 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 too 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.

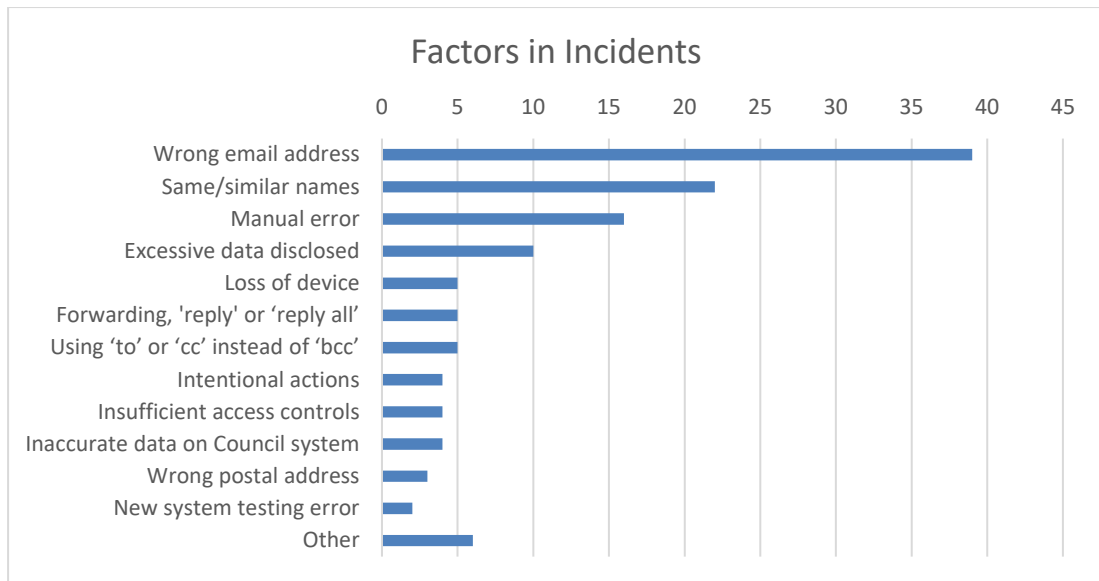
Over the course of 2022, the Council recorded 54 Data Breaches and 24 Near Misses, resulting in a total of 78 incidents. These incidents occurred across Council Divisions as follows:



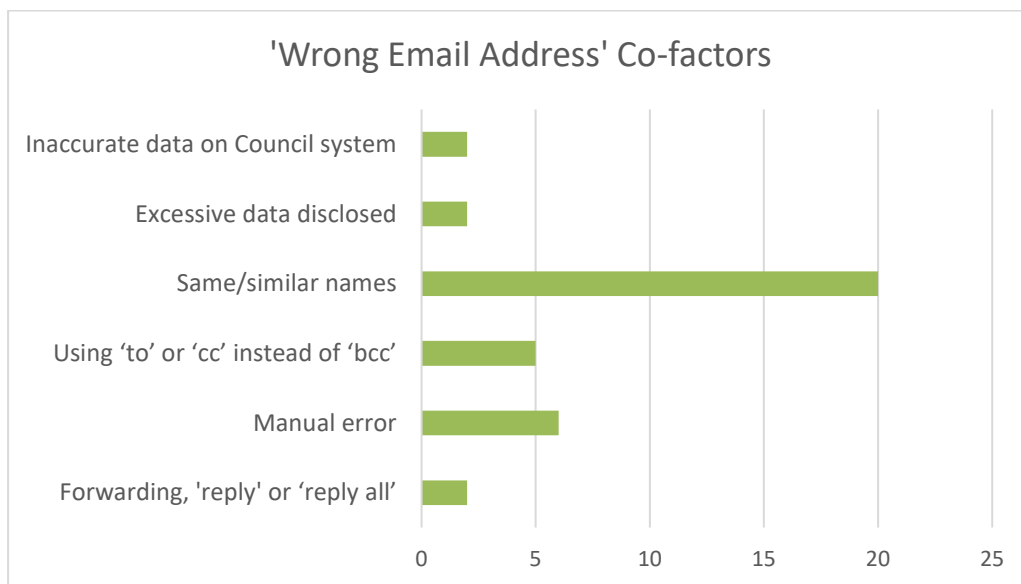
- 3.9 A total of **three** incidents were considered to meet the ‘likely risk’ threshold for reporting to the Information Commissioner’s Office. In all three cases, the ICO found that the Council had appropriate technical and organisational measures in place, and took no further action.
- 3.10 No incidents were considered to meet the statutory ‘high risk’ threshold requiring reporting to the Data Subject(s), however in some cases Council officers chose to inform the Data Subject(s) as a point of good practice.
- 3.11 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. On one occasion, a third party Supplier was subject to a cyber-attack that compromised Council-controlled data, however on investigation this was found to present low risk to East Lothian clients/customers.
- 3.12 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.



- 3.13 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 **39** instances.



3.14 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':



3.15 Regarding the three breaches reported to the ICO, contributing factors included:

- Wrong email address
- Using 'to' or 'cc' instead of 'bcc'
- Disclosure of excessive data
- New system testing error

Lessons learned

- 3.16 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.
- 3.17 In relation to incidents reported to the ICO, the Council was found to have appropriate technical and organisational measures in place. In their responses, the ICO noted a number of areas of good practice, as well as recommended actions. Combined feedback from the ICO and the Council's Internal Audit Service regarding the Council's overall Data Protection Compliance is set out in the following table, along with the actions taken in 2022 and planned measures for 2023:

Good Practice
<p><i>Information Commissioner's Office</i></p> <ul style="list-style-type: none"> • Preventative measures in place, including a Data Protection Impact Assessment, Data Protection Policy, IT Accessible Use Policy, and Data Protection training for all staff; • Review/testing of new systems before implementation; • Remedial action taken immediately to contain incidents; • Ongoing discussion/work with partner organisations to implement prevention of incident recurrence.
<p><i>Internal Audit</i></p> <ul style="list-style-type: none"> • Clearly defined policies, procedures, guidance, roles and responsibilities; • Appropriate use of Privacy Notices; • Appropriate arrangements for data sharing, including Data Sharing Agreements with third parties; • Appropriate procedures for responding to, documenting and reporting Data Breaches / Near Misses; • Regular reporting of data protection risks to senior managers; • Appropriate data protection training; • Appropriate input into COVID-19 response.
Recommendations
<p><i>Information Commissioner's Office</i></p> <ul style="list-style-type: none"> • Review internal security procedures to identify additional preventative measures; • Spot-checking systems to ensure they are robust and fit for purpose; • Continue to monitor incidents for evidence of additional risk/detriment to Data Subjects;
<p><i>Internal Audit</i></p> <ul style="list-style-type: none"> • Seek to ensure that relevant policies and procedures are reviewed on a regular basis;

<ul style="list-style-type: none"> • 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.
<p>Actions Taken</p> <ul style="list-style-type: none"> • Additional Information Officer recruited to post in early December 2022; • Additional Team Lead-Information Governance post creation in progress; • Access procedures for the Council's Social Work case management system, Mosaic, reviewed; • 19 Data Sharing Agreements reviewed and signed; 39 in progress, 1 declined. • 11 Data Protection Impact Assessments reviewed and signed off; 38 in progress. • New and streamlined review/authorisation procedures have been designed for Data Sharing Agreements ('DSAs') and Data Protection Impact Assessments ('DPIAs'); • Reports on compliance scheduled to be submitted annually to Audit and Governance Committee;
<p>Planned Actions</p> <ul style="list-style-type: none"> • Communications/Training Plan development to be led by new Team Lead-Information Governance pending recruitment; • Information Asset Register workshops to be conducted quarterly, supported by new Information Officer; • Information Champions to be identified within each Service in line with completion of the Information Asset Register; • Backlog of DSAs and DPIAs to be addressed in line with new procedures, supported by new Team Lead pending recruitment.

3.18 Noting the correlation between the number of email-related data incidents and factors involving human errors, it is predicted that an increased focus on training and awareness of Data Protection across Services via the Communications/Training Plan will be key to improving compliance in relation to data breaches going forward.

Records Management

3.19 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.

- 3.20 The Keeper's Assessment Team's full comments on the Council's 2022 annual review are provided as a Background Paper to this report.
- 3.21 Additionally, the Council Management Team ('CMT') has recently taken a major step forward for Records Management compliance by giving approval to contract out all storage, retrieval and destruction services for paper records. A procurement exercise will be performed by the end of financial year 2022-23 to identify a best value Supplier, 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.
- 3.22 The Council's Records Management Plan is modelled after the Keeper's Model Plan, which at the time of creation included 14 Elements. Key updates in relation to these Elements include:

- Elements 4 & 5 – Business Classification Scheme (BCS) / Retention Schedule

The Council has retired the previous version of the BCS / Retention Schedule and adopted the current version of the national model Retention Schedules produced by the Scottish Council on Archives ('SCARRS'), which are available to all staff via the Council intranet.

Initial steps have been taken to implement Microsoft 365 ('M365'), with a view to wider roll-out throughout the Council over 2023 and beyond. The Information Governance features of M365 are robust, and will allow the automatic application of Retention labels to individual records belonging to all Council Services. This is a key step in practically applying the BCS and Retention Schedule to the Council's records, and will provide a significant improvement to compliance in relation to digital records.

- Element 6 – Destruction

The introduction of M365 will also bring significant improvement to the Council's arrangements for the secure destruction of digital records. M365 allows for records to be regularly reviewed and authorised for destruction based on Retention labels; it also allows 'holds' to be applied to specific records or types of records to ensure they are not destroyed, even if their Retention period has expired.

As the Council increasingly shifts to digital ways of working, these features will become a key component of the Council's compliance with this Element.

- Element 7 – Archiving and Transfer

Following recruitment of an additional Information Officer in early December 2022, work has commenced to scope and create a Digital Preservation Plan to ensure that our records of enduring business and historical value remain accessible and retain their integrity.

- Element 10 – Business Continuity

The transfer of paper records to an external Supplier will improve environmental conditions and controls for records storage. Professional-level protection against fire, flood and other disasters will help to ensure that the Council's paper information assets remain usable and accessible, and this will also mitigate the risk of personal data breaches due to data loss.

- Element 11 – Audit Trail

As part of the services offered by the new Supplier, Council staff will have the option of requesting files to be delivered to Council premises within 1 week, 1 day, a half day or 2 hours. They will also have the option to request that records be scanned and sent to the requester as digital files or made accessible via an online portal ('scan on demand').

The movements of any paper file between storage and Council premises will be tracked, with an audit trail retained. Likewise any action performed against a record, such as modification of metadata, added/removed files, and permanent destruction will be recorded and tracked, and certificates of destruction will be issued. Access to records will be role-based and strictly controlled, thus reducing the risk of data breaches due to unauthorised access.

This will be a significant improvement to the Council's current file tracking and access controls, which are currently manual and very limited.

- Element 15 – Public Records Created by Third Parties

The Keeper's Model Plan states that 'adequate arrangements must be in place for the management of records created and held by third parties who carry out any functions of the Council.' This Element was introduced to the Model Plan by the Keeper in 2019, therefore it is not present in the Council's current Records Management Plan, which was first implemented in 2015. Work is ongoing to gather relevant information to evidence the Council's compliance with this Element as part of a future re-submission to the Keeper.

Covert Surveillance

- 3.23 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').

- 3.24 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.
- 3.25 East Lothian Council has to-date made very limited use of its RIPSA powers, and there were no applications made in 2022.
- 3.26 In February/March 2022, the Council underwent a desktop inspection by the Investigatory Powers' Commissioner's Office ('IPCO'), the national regulator for compliance with the RIPSA framework (RIPA in England and Wales). The inspection was in line with the routine 3-yearly inspection schedule for relevant authorities, and consisted of a video conference interview involving the Inspector, the Council's Senior Responsible Officer (Head of Corporate Support), the RIPSA Gatekeeper / Coordinating Officer (Team Manager-Information Governance) and the Service Manager-Governance. The Inspector provided comments on the Council's RIPSA documentation over the period 2018-2021 and asked the Council officers a series of questions, noting that the level of compliance shown by the Council removed the need for a physical inspection.
- 3.27 The Inspector's report was positive on the whole, noting a number of points of good practice, and including recommendations for improvements.

Good Practice
<ul style="list-style-type: none"> • Introduction of quality assurance process for RIPSA applications; • Development of a training programme for relevant Council officers, including a new 'Guide for Authorising Officers'.
Recommendations
<ul style="list-style-type: none"> • Update RIPSA Policies and submit to Elected Members at least once a year; • Authorising Officers must not attempt to adjust 3-month authorisation periods; • Ensure applicants do not conflate considerations of necessity and proportionality; • Include sufficient considerations of collateral intrusion by applicants and Authorising Officers.
Actions Taken
<ul style="list-style-type: none"> • RIPSA and Surveillance Through Social Media Policies were combined into a single RIPSA Policy and approved by Cabinet on 14 June 2022; • Reports on compliance scheduled to be submitted annually to Audit and Governance Committee;

<ul style="list-style-type: none"> • Guidance for Authorising Officers updated.
<p>Planned Actions</p> <ul style="list-style-type: none"> • RIPSAs 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 RIPSAs material; • E-learning module to be developed; • Service Manager-Governance to undertake external training.

2023: Information Transformation Strategy

- 3.28 Looking forward, a key focus of 2023 will be the development of an Information Transformation Strategy. The Strategy will underpin and support the provisions of the new Digital Strategy, and will draw together the elements and considerations set out in this report with an overall aim of getting the right information to the right person, at the right time, and in the right format.
- 3.29 The rapid changes to working practices that were triggered and accelerated by the COVID-19 pandemic are now embedded in the Council's ways of working, with customer expectations and compliance demands higher than ever. By adopting a Customer First, responsive approach to information management as an integral component of our wider business strategies, we can ensure effective decision-making based on robust and reliable data, all while protecting individual rights, maintaining compliance and preserving the Council's legacy in its communities.

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 Progress Update Review (PUR) Report by the PRSA Assessment Team (01 November 2022)
- 6.2 East Lothian Council Data Protection Audit Report (November 2022)
- 6.3 IPCO CHIS and Surveillance Inspection of East Lothian Council (08 March 2022)

AUTHOR'S NAME	Zarya Rathé
DESIGNATION	Team Manager-Information Governance
CONTACT INFO	zrathe@eastlothian.gov.uk ; 01620 827989
DATE	31/01/2023

APPENDIX 1

Legislation	Key Features
Data Protection Act 2018 / UK GDPR	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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; • RIPSAs 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.

The Public Records (Scotland) Act 2011

East Lothian Council and Licensing Board

Progress Update Review (PUR) Report by the PRSA Assessment Team

01 November 2022

Contents

1. The Public Records (Scotland) Act 2011.....	3
2. Progress Update Review (PUR) Mechanism.....	4
3. Executive Summary.....	5
4. Authority Background.....	5
5. Assessment Process.....	6
6. Records Management Plan Elements Checklist and PUR Assessment.....	7-22
7. The Public Records (Scotland) Act Assessment Team's Summary.....	23
8. The Public Records (Scotland) Act Assessment Team's Evaluation.....	24

1. Public Records (Scotland) Act 2011

The Public Records (Scotland) Act 2011 (the Act) received Royal Assent on 20 April 2011. It is the first new public records legislation in Scotland since 1937 and came into force on 1 January 2013. Its primary aim is to promote efficient and accountable record keeping by named Scottish public authorities.

The Act has its origins in *The Historical Abuse Systemic Review: Residential Schools and Children's Homes in Scotland 1950-1995* (The Shaw Report) published in 2007. The Shaw Report recorded how its investigations were hampered by poor recordkeeping and found that thousands of records had been created, but were then lost due to an inadequate legislative framework and poor records management. Crucially, it demonstrated how former residents of children's homes were denied access to information about their formative years. The Shaw Report demonstrated that management of records in all formats (paper and electronic) is not just a bureaucratic process, but central to good governance and should not be ignored. A follow-up review of public records legislation by the Keeper of the Records of Scotland (the Keeper) found further evidence of poor records management across the public sector. This resulted in the passage of the Act by the Scottish Parliament in March 2011.

The Act requires a named authority to prepare and implement a records management plan (RMP) which must set out proper arrangements for the management of its records. A plan must clearly describe the way the authority cares for the records that it creates, in any format, whilst carrying out its business activities. The RMP must be agreed with the Keeper and regularly reviewed.

2. Progress Update Review (PUR) Mechanism

Under section 5(1) & (2) of the Act the Keeper may only require a review of an authority's agreed RMP to be undertaken not earlier than five years after the date on which the authority's RMP was last agreed. Regardless of whether an authority has successfully achieved its goals identified in its RMP or continues to work towards them, the minimum period of five years before the Keeper can require a review of a RMP does not allow for continuous progress to be captured and recognised.

The success of the Act to date is attributable to a large degree to meaningful communication between the Keeper, the Assessment Team, and named public authorities. Consultation with Key Contacts has highlighted the desirability of a mechanism to facilitate regular, constructive dialogue between stakeholders and the Assessment Team. Many authorities have themselves recognised that such regular communication is necessary to keep their agreed plans up to date following inevitable organisational change. Following meetings between authorities and the Assessment Team, a reporting mechanism through which progress and local initiatives can be acknowledged and reviewed by the Assessment Team was proposed. Key Contacts have expressed the hope that through submission of regular updates, the momentum generated by the Act can continue to be sustained at all levels within authorities.

The PUR self-assessment review mechanism was developed in collaboration with stakeholders and was formally announced in the Keeper's Annual Report published on 12 August 2016. The completion of the PUR process enables authorities to be credited for the progress they are effecting and to receive constructive advice concerning on-going developments. Engaging with this mechanism will not only maintain the spirit of the Act by encouraging senior management to recognise the need for good records management practices, but will also help authorities comply with their statutory obligation under section 5(1)(a) of the Act to keep their RMP under review.

3. Executive Summary

This Report sets out the findings of the Public Records (Scotland) Act 2011 (the Act) Assessment Team's consideration of the Progress Update template submitted for East Lothian Council and Licensing Board. The outcome of the assessment and relevant feedback can be found under sections 6 – 8.

4. Authority Background

East Lothian borders the City of Edinburgh, Midlothian and the Scottish Borders. Its administrative centre is Haddington, although its largest town is Musselburgh.

The council area was created in 1996, replacing the East Lothian district of the Lothian region. The district had been created in 1975 under the Local Government (Scotland) Act 1973, consisting of the old county of East Lothian plus the burghs of Musselburgh and Inveresk, which until then had been in the county of Midlothian.

Licensing is the responsibility of licensing boards under powers contained in the Licensing (Scotland) Act 2005. Local licensing boards have wide discretion to determine appropriate licensing arrangements according to local needs and circumstances and their own legal advice. Each local government area must have a licensing board. East Lothian Licensing Board consists of 6 Board members.

5. Assessment Process

A PUR submission is evaluated by the Act's Assessment Team. The self-assessment process invites authorities to complete a template and send it to the Assessment Team one year after the date of agreement of its RMP and every year thereafter. The self-assessment template highlights where an authority's plan achieved agreement on an improvement basis and invites updates under those 'Amber' elements. However, it also provides an opportunity for authorities not simply to report on progress against improvements, but to comment on any new initiatives, highlight innovations, or record changes to existing arrangements under those elements that had attracted an initial 'Green' score in their original RMP submission.

The assessment report considers statements made by an authority under the elements of its agreed Plan that included improvement models. It reflects any changes and/or progress made towards achieving full compliance in those areas where agreement under improvement was made in the Keeper's Assessment Report of their RMP. The PUR assessment report also considers statements of further progress made in elements already compliant under the Act.

Engagement with the PUR mechanism for assessment cannot alter the Keeper's Assessment Report of an authority's agreed RMP or any RAG assessment within it. Instead the PUR Final Report records the Assessment Team's evaluation of the submission and its opinion on the progress being made by the authority since agreeing its RMP. The team's assessment provides an informal indication of what marking an authority could expect should it submit a revised RMP to the Keeper under the Act, although such assessment is made without prejudice to the Keeper's right to adopt a different marking at that stage.

Key:

G	The Assessment Team agrees this element of an authority's plan.	A	The Assessment Team agrees this element of an authority's progress update submission as an 'improvement model'. This means that they are convinced of the authority's commitment to closing a gap in provision. They will request that they are updated as work on this element progresses.	R	There is a serious gap in provision for this element with no clear explanation of how this will be addressed. The Assessment Team may choose to notify the Keeper on this basis.
----------	---	----------	---	----------	--

6. Progress Update Review (PUR) Template: East Lothian Council and Licensing Board

Element	Status of elements under agreed Plan 05JAN15	Progress Status 17JUL19	Progress Status 01NOV22	Keeper's Report Comments on Authority's Plan 05JAN15	Self-assessment Update 15MAY19	Progress Review Comment 17JUL19	Self-assessment Update as submitted by the Authority since 17JUL19	Progress Review Comment 01NOV22
1. Senior Officer	G	G	G	Update required on any change.	No Change.	No immediate action required. Update required on any future change.	The Council officer holding Senior Management responsibility for the Records Management Plan is now Morag Ferguson, Head of Corporate Support, mferguson@eastlothian.gov.uk.	The Assessment Team thanks you for this update which has been noted. Update required on any change.
2. Records Manager	G	G	G	Update required on any change.	East Lothian Council appointed Zarya Rathé as Team Manager for Information Governance and Data Protection in 2018. Due to maternity leave commencing in October 2018 Maureen Henderson was appointed interim Team Manager for Information Governance and Data	The Assessment Team thanks East Lothian Council for this update which we have noted.	Zarya Rathé has resumed her post as Team Manager-Information Governance (and Data Protection Officer).	Thank you for this update which has been noted. Update required on any future change.

					Protection.			
3. Policy	G	G	G	Update required on any change.	<p>No change has taken place due to the implementation of GDPR and other priorities so the review of the Information and Records Management Policy has not been done at this present moment but works is currently about start as it's been decided that a rewrite is required of East Lothian Council Records Management Plan which will coincide with the Launch of the new Records Management Plan.</p>	<p>The Keeper's Assessment Team note the Council intends to review and update their Records Management Plan (see element 13 below). This is apparent in the PUR text for several elements below and will be an important step going forward.</p> <p>The Act requires an authority to keep its Records Management Plan under review and this is a good indication that East Lothian Council is committed to complying with this aspect of the legislation. They look forward to being kept updated on this work in subsequent PURs.</p>	<p>Formal review of the Council's RMP has slowed since the activation of the Council's Business Continuity measures in March 2020, which limited activities to business-critical operations only. While these measures currently remain in effect, the Council is now looking toward recovery and we expect to progress toward our aim of developing and re-submitting a fresh RMP to the Keeper for assessment in the coming year. Formal review and approval of an up-to-date Information and Records Management Policy will be included in that process.</p> <p>The Council is also in the early stages of developing an Information Transformation Strategy to address the holistic management of Council information across formats, systems and platforms. The Strategy</p>	<p>Thank you for letting the Assessment Team know that that the Records Management Plan (RMP) review process has slowed down due to the impact of the pandemic and the prioritisation of business-critical operations.</p> <p>The receipt of evidence provided is acknowledged with thanks. The Report on the RMP progression, in particular, highlights East Lothian Council and LB's commitment to complying with PRSA, and it is hoped this results in a robust RMP submission for The Keeper's assessment. The Information</p>

						<p>The PUR notes that, because of this review, there has been some slippage in the review dates of other information governance documents (The Records Management Policy particularly). This is to be expected.</p> <p>The Keeper accepts that the current Records Management Policy is operational until superseded. However, if this were a formal re-submission under section 5 of the PRSA, the RM Policy would have to be 'in-date' to attain the Keeper's agreement.</p>	<p>will underpin the Council's Digital Strategy and Business Transformation agendas; we aim to complete this early in 2023, dependent on completion of the Digital Strategy, expected around the end of 2022.</p> <p>The Council's Information Governance team is also in the process of reviewing and updating its suite of Records Management and Archives guidance which is published on the Council Intranet.</p> <p>Supporting evidence:</p> <ul style="list-style-type: none"> • Report presented to the Council's Policy and Performance Review Committee regarding progression of the RMP; • Briefing Note re: Information Transformation Strategy 	<p>Transformation Strategy and the review of guidance for staff will positively contribute to this process.</p> <p>See also Element 13.</p>
4. Business Classification	A	A	A	The Keeper would like to know when this survey is complete and potentially view	No change – work continues on the BCS but due to the RM manager leaving and other priorities but East Lothian Council	The BCS roll-out continues. The roll out of this major piece of work is bound to be incremental	The Council is currently undertaking an Asset Review project, addressing the consolidation of the	The Assessment Team thanks you for this update on the ongoing Asset Review project and

				<p>the 'targeted plan for implementation of classification scheme.'</p> <p>The Keeper requests that he is kept informed on the development of the proposal and that he may view the outcome of the "EDRMS Review" planned for 2015. He would be especially interested in information regarding any alternative solution should the CIVICA proposal be rejected.</p> <p>The RMP indicates that a restructuring of paper file store 'may' be undertaken. The Keeper will be</p>	<p>are committed to carrying on this work and implement the BCS standard throughout the council.</p> <p>EDRMS is still being looked into by East Lothian Council.</p> <p>No change to the paper filing system but as paper files are still generated and East Lothian Council still have legacy paper files this will form part of the EDRMS project which will look at options for the paper records going forward.</p> <p>No changes have been made to the naming guidance.</p>	<p>and further time must be allowed for it to bed in and become fully operational. This element remains at 'amber' for the moment as the work progresses.</p> <p>The Assessment Team notes the update of the EDRMS project and look forward to being kept updated on this work in subsequent PURs.</p>	<p>Council estate in line with changing ways of working. To support the closure and re-allocation of office space, the Council's Information Governance team is supporting individual Services via a series of mini-Record Audits, addressing the extent of paper records held in offices and identifying anticipated needs in terms of retention, storage and scanning. As part of this process, Services are also being encouraged to set up and enforce agreed File Plans in line with refreshed guidance and tied to the Council's BCS (see below).</p> <p>The Council has also continued to progress development of its Information Asset Register via an ongoing series of workshops with individual Service areas. As part of these workshops, Services are asked to review their record holdings against</p>	<p>the mini- Record Audits. It is also positive to hear that File Plan guidance has been updated and Services encouraged (although, it is noted, not required) to use these as they tie into the Council's Business Classification Scheme. The Assessment Team would like to ask if this means the BCS has now been fully implemented and is operational.</p> <p>The development of the Information Asset Register, and how this ties up with the BCS, is also noted with thanks.</p> <p>Thank you for submitting supporting evidence, the receipt of which is acknowledged.</p>
--	--	--	--	---	---	--	--	---

				<p>interested to know what decision is taken regarding this.</p>			<p>the BCS and Retention Schedule and link individual Information Assets to the appropriate entries on the BCS/Retention Schedule (and/or develop new entries/retention rules as required in conjunction with the Information Governance team).</p> <p>File Naming and File Planning guidance has recently been updated and distributed to Services which are currently participating in the Asset Review project. This will be made available to all staff via the Council Intranet shortly.</p> <p>Supporting evidence:</p> <ul style="list-style-type: none"> • Sample Record Audit questionnaire; • Sample IAR entries; • File Naming Guidelines; • File Planning Principles <p>Update in October 2022: We would not characterise the BCS as fully implemented at this</p>	<p>Whilst progress has been made, this Element remains at Amber as the work continues. The Team look forward to a more comprehensive indication of the authority's position in the planned voluntary RMP resubmission.</p> <p>Comments on further update: The Assessment Team is grateful for the clarification provided. It is good to hear of the changed approach to BCS.</p>
--	--	--	--	--	--	--	---	---

							stage. Since our initial PUR submission in April, we have since taken a decision to replace use of the LGCS with use of the inherent BCS in the SCA BCS/RRS model Retention Schedules, and to update our Retention Schedule in line with revision schedule for the national model Schedules which are currently under review by the Scottish Council on Archives, with ongoing engagement with local authorities to be facilitated by a dedicated SCARRS Sub-group within the Archivists of Local Authorities Working Group (ASLAWG) which has been recently established. There will need to be updates made accordingly to the Council's existing Information Asset Register entries.	
5. Retention Schedule	A	A	A	The Keeper requires East Lothian Council to keep him up to date on	No change to the current status of destruction and the 2018 deadline has been missed, but as part of the rewrite of	The BCS/Retention Schedule roll-out continues. The roll out of this major piece of	Updates and revisions to the Retention Schedule continue, with particular focus on areas affected by the Asset Review over	Thank you for this update regarding ongoing work on updating and revising the

				<p>progress.</p>	<p>the Records Management Plan the retention schedule document will be reviewed.</p>	<p>work is bound to be incremental and further time must be allowed for it to bed in and become fully operational. This element remains at 'amber' for the moment as the work progresses. The PUR also notes that, because of the Records Management Plan review, and other issues affecting the Council in the last 12 months, there has been some slippage in the review dates of other information governance documents (The Retention Schedule). This is to be expected.</p>	<p>the next 6 months.</p> <p>Records disposal modules have been introduced in systems used by Revenues/Benefits, HR/Payroll and Housing, although further work continues to be required to address application of retention rules to digital records across Council systems.</p> <p>As the Information Asset Register develops, the Council is looking at use of the IAR as a tool for addressing regular review of information assets with reference to the Retention Schedule. It should be noted that this is currently in an exploratory phase and has not yet been formally adopted.</p>	<p>Retention Schedule. This is a key element in the practical implementation of records retention procedures, and allows for organisation-wide, consistent application of rules.</p> <p>The update mentions digital records retention rules and indicates that electronic records retention procedures are not fully in place. This is a cause for concern as the proportion of digital records over paper records has, as a general trend, been gradually increasing every year.</p> <p>Thank you also for informing the Assessment Team of the exploratory project of using the IAR as a tool to</p>
--	--	--	--	------------------	--	--	---	--

								<p>address regular review of information assets.</p> <p>This Element will remain at Amber as the improvements requested by the Keeper have not yet been implemented. We look forward to hearing more about this in the upcoming voluntary RMP resubmission.</p>
6. Destruction Arrangements	A	A	A	<p>The Council is planning to set protocols for the use of internal shredders. The Keeper requests sight of these protocols when they are available.</p> <p>Electronic Records Destruction. The Keeper accepts that the Council has properly</p>	<p>No Change but will be consider during the rewrite of the Records Management Plan.</p>	<p>Along with many other Scottish public authorities the controlled, timely and secure destruction of digital records remains a potential weakness. East Lothian Council will be in a better position to address this when the BCS/Retention Schedule is fully implemented. This element remains at</p>	<p>The Council's arrangements for the destruction of paper records, including the engagement of external Suppliers of document management services, are currently under review. As part of the Information Transformation Strategy, we intend to set the future aims and direction for paper records management with consideration for the changing use of the Council estate and the</p>	<p>The Assessment Team thanks you for this update on records destruction arrangements. It is acknowledged that the Council's arrangements with regard to paper records are currently under review.</p> <p>It is noted that records destruction of electronic records remains unchanged.</p>

				identified a gap in provision and has appropriate mechanisms in place to close that gap.		'amber' for the moment as this work progresses. The Assessment Team acknowledges the planned development of a new Records Management Plan. They look forward to being kept updated on record destruction provision in subsequent PURs.	recent introduction of a new Home Working Policy and associated provisions. There have been no significant changes to the Council's provisions for electronic destructions, however work is planned regarding the implementation of EDRMS and exploring use of the Information Asset Register as another tool for managing destructions across formats.	The Team would like to remind East Lothian Council and Licensing Board that the implementation of EDRMS will also have major implications on the records destruction procedures, as well as Elements 4, 5 and 11. It appears work continues. This Element will remain at Amber until this has been completed, but the implementation of EDRMS may require that approach to this Element's practical implementation is reconsidered.
7. Archiving and Transfer	G	G	G	The Keeper requests the two new documents (Acquisitions Policy & Transfer	No change but the policy will be reviewed during the re-write of the Records Management Plan.	No immediate action required. Update required on any future change. The Assessment Team	No change, but Digital Preservation will be included as a key component of the Information Transformation Strategy.	Thank you for letting the Assessment Team know that there have been no major changes to

				Procedures) planned relating to the management of archival material are forwarded to him when appropriate.		acknowledges the planned development of a new Records Management Plan. They look forward to being kept updated on this work in subsequent PURs.		East Lothian Council and Licensing Board's archiving and transfer arrangements. That focus on digital preservation as a key component of the Information and Transformation Strategy is also noted with thanks.
8. Information Security	G	G	G	The Keeper requests that if any changes occur as part of the review of the Information Security Policy in December 2015 that he is provided with an updated version.	No change but the policy will be reviewed during the rewrite of the Records Management Plan.	No immediate action required. Update required on any future change. The Assessment Team acknowledges the planned development of a new Records Management Plan. They look forward to being kept updated on this work in subsequent PURs.	Updates are in progress to the Council's IT Acceptable Use Policy, which is expected to be finalised and implemented imminently.	Thank you for this update on the IT Acceptable Use Policy review. This is one of a suite of documents that will assist East Lothian Council and LB keep adequate procedures in place to protect their records against unauthorised access, alteration, destruction, or removal of records, and the Team trusts that other policies, including the Information Security Policy, are regularly reviewed

								and kept up to date.
9. Data Protection and 14. Shared Information	G	G	G	<p>The Keeper requests that he is provided with the Board's registration number when it becomes available.</p> <p><i>East Lothian Council and Licensing Board have opted to consider both of these Elements together under Element 9. On Shared Information (Element 14), update is required on any change.</i></p>	<p>A lot of change under this element due to the implementation of new Data Protection Legislation, so East Lothian Council have concentrated on updating guidance and this is evidence from E01-E07 and this information has been made available to staff and schools. We have also still been engaging with schools and attending meetings answering any relevant questions or concerns in relation to the new Data Protection Legislation. We are also midst drafting a Social Media policy for schools so they understand the rules in regards to social media in relation to children.</p> <p>We are also in the middle of renewing and updating our Data Sharing Agreements (E08) and Data Processing</p>	<p>As with all other Scottish public authorities East Lothian Council have been required to review and update their data protection procedures in light of the 2018 legislation. The Assessment Team acknowledge receipt of a suite of new GDPR compliant data protection policy and guidance documents. These will be stored to keep the East-Lothian Council submission up to date.</p> <p>The Assessment Team acknowledges the receipt of a screen-shot showing staff have access to the new GDPR staff guidance</p>	<p>Updates to policies, procedures and templates have been progressed to reflect that, following Brexit, personal data processing in the UK is now governed by the UK GDPR. Existing templates for Data Sharing Agreements, Data Protection Impact Assessments and wording within the Council's standard Terms and Conditions are also under review with reference to national and regional frameworks.</p> <p>Update in October 2022: The Council's template Data Sharing Agreements have been updated as required since the approval of East Lothian Council's RMP in 2015. The most significant changes to existing templates were in 2018 to bring these in line with the requirements of the Data Protection Act 2018 and</p>	<p>Thank you for this update on ensuring that policies and templates reflect the most recent legislative framework in place. This is a key requirement under Element 9.</p> <p>Regarding Element 14, the Team assumes no changes to existing Data Sharing Agreements have taken place, and that these Agreements are being kept up to date and relevant for their purpose.</p> <p>Comments on further update: Thank you for taking the time to confirm that Data Sharing Agreement templates have</p>

					<p>Agreements we have with suppliers and others so we are fully aware of who we are sharing information, ELC are also developing a register of these agreements which will hopefully linked to the Information Asset register and any relevant Data Protection Impact Assessments but all this is still in development but will be updated in rewrite of the Records Management Plan.</p>	<p>documents. The Assessment Team also note the updated information on the East Lothian Council website: https://www.eastlothian.gov.uk/info/2/10598/access_to_information/12340/privacy_and_cookies</p>	<p>the GDPR. Relevant updates have continued to be made, for example to reflect the implementation of the UK GDPR following the UK's withdrawal from the EU. The total number of Data Sharing Agreements in place for the Council's routine data sharing activities has significantly increased since 2015 and in particular since May 2018 when the Data Protection Act 2018 / GDPR came into effect.</p>	<p>been updated.</p>
10. Business Continuity and Vital Records	A	G	G	<p>The Keeper requires that the Council provide him with a redacted sample of a Service Business Continuity Plan when they are completed.</p>	<p>East Lothian Council have recently published an updated Business Continuity Plan and is evidenced at E09.</p>	<p>The Assessment Team acknowledge the receipt of the East Lothian Council Business Continuity Plan (v1.0) dated January 2019. As noted in previous PUR, the Assessment Team recognises the significant progress made in this area and the on-going initiative being undertaken</p>	<p>No change.</p> <p>Update in October 2022: The current ongoing record audits are linked to the Council's Asset Review programme, through which Council buildings are being cleared and re-purposed as more flexible working spaces. While this programme was and is not directly driven by the Council's pandemic response, it has certainly</p>	<p>Thank you for letting the Assessment Team know there have been no major updates to Business Continuity arrangements. However, as this is the first update following the pandemic, the Team would have liked to hear how the authority's business continuity</p>

						<p>by the authority under this element. It is likely that if this were a formal re-submission under section 5 of the PRSA this element would gain a 'Green' RAG status.</p>	<p>grown and accelerated due to the changes to ways of working that were catalysed by the pandemic. A new Home Working Policy, for example, was introduced in April 2022, allowing employees to apply for contractual working-from-home arrangements, which has and will continue to reduce demand on office space, as well as introducing new challenges regarding records management and information security/data protection. Guidance on working safely from home while protecting personal information and managing records properly was developed near the start of the pandemic, and will continue to evolve in line with the preparation of the Council's second Records Management Plan.</p> <p>Our Business Continuity software was used throughout the pandemic as well as an ongoing spreadsheet detailing where each service was</p>	<p>processes fared during the disruption, and if any reviews to these are planned as a result.</p> <p>Under Element 4, the Council and Licensing Board noted that mini Record Audits were taking place, 'addressing the extent of paper records held in offices and identifying anticipated needs in terms of retention, storage and scanning.' The Team would be interested to clarify if these records relate to changed ways of working during the pandemic, or if this action is taking place as business as usual.</p> <p>Comments on further update:</p>
--	--	--	--	--	--	---	---	--

							at as regards BC. The BC software provide invaluable and was used by CMT to get a picture of the Council's BC response. Services which remain in BC mode remain invoked on the software. The only review would be to update all BC SPoCs [Single Points of Contact] on use of the software.	The Assessment Team is grateful for this clarification, and further information on Business Continuity Arrangements
11. Audit Trail	A	A	A	The Keeper requests that he is kept up to date with the project as it progresses.	No change.	No immediate action required. Update required on any future change. East Lothian Council will be in a better position to address this when the BCS/Retention Schedule is fully implemented.	As part of the Asset Review, the Council is taking steps to standardise the metadata applied to paper records and to enhance file tracking through the engagement of an external contractor. Control of digital records is continuing to develop as staff identify information flows via the Information Asset Register.	The Keeper will expect authorities to maintain a complete and accurate representation of all changes that occur in relation to a particular records. This includes changes to the record's location, both in relation to analogue and digital records.
12. Competency Framework	G	G	G	Update Required on Any Change.	No change.	No immediate action required. Update required on any future change.	No change.	It is important that staff training requirements are reviewed regularly

								<p>as systems or way of working (e.g. working from home) change so that staff continue to be adequately supported in their adherence to the authority's RMP.</p> <p>Update required on any change.</p>
13. Assessment and Review	G	G	A	<p>The Keeper requests that if any changes result from the review he is provided with the updated version.</p> <p>The Keeper would be interested in the results of the Data Protection Health Check, if appropriate.</p>	<p>East Lothian Council have made the decision with the launch of the new Records Management Plan that they are going to do a re-write of the Records Management Plan this year.</p>	<p>Once the Records Management Plan has been revised and updated, the Council may choose to re-submit formally under section 5 of the Act. This would be welcomed.</p>	<p>No change.</p>	<p>East Lothian Council and Licensing Board should be commended for their regular participation in the PUR process (in 2016, 2017, 2019 and 2022).</p> <p>While no update has been given here regarding Element 13, Element 3 suggests that the pandemic-related delays have caused significant delay to the regular review and update process of the RMP</p>

								<p>and some adjacent policies.</p> <p>This Element has been changed from Green to Amber to indicate that the authority has not been able to keep focus on this Element while resource has been redeployed due to the pandemic. We acknowledge, however, that they are taking active steps to rectify this.</p>
14. Shared Information				<p>See element 9. East Lothian Council and Licensing Board have opted to consider both of these Elements together under Element 9.</p>				

7. The Public Records (Scotland) Act Assessment Team's Summary

Version

The progress update submission which has been assessed is the one received by the Assessment Team on 18 May 2022. The progress update was submitted by Zarya Rathé, Team Manager and Information Governance and Data Protection Officer.

The progress update submission makes it clear that it is a submission for **East Lothian Council and Licensing Board**.

The Assessment Team has reviewed East Lothian Council and Licensing Board's Progress Update submission and agrees that the proper record management arrangements outlined by the various elements in the authority's plan continue to be properly considered. The Assessment Team commends this authority's efforts to keep its Records Management Plan under review.

General Comments

East Lothian Council and Licensing Board continues to take its records management obligations seriously and is working to bring all elements into full compliance.

Section 5(2) of the Public Records (Scotland) Act 2011 provides the Keeper of the Records of Scotland (the Keeper) with authority to revisit an agreed plan only after five years has elapsed since the date of agreement. Section 5(6) allows authorities to revise their agreed plan at any time and resubmit this for the Keeper's agreement. The Act does not require authorities to provide regular updates against progress. The Keeper, however, encourages such updates.

The Keeper cannot change the status of elements formally agreed under a voluntary submission, but he can use such submissions to indicate how he might now regard this status should the authority choose to resubmit its plan under section (5)(6) of the Act.

8. The Public Records (Scotland) Act Assessment Team's Evaluation

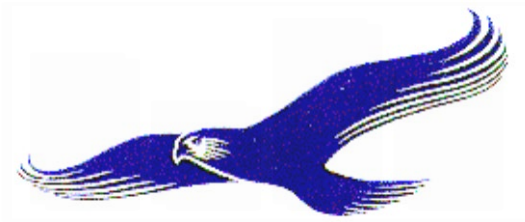
Based on the progress update assessment the Assessment Team considers that East Lothian Council and Licensing Board continue to take their statutory obligations seriously and are working hard to bring all the elements of their records management arrangements into full compliance with the Act and fulfil the Keeper's expectations.

The Assessment Team recommends authorities consider publishing PUR assessment reports on their websites as an example of continued good practice both within individual authorities and across the sector.

This report follows the Public Records (Scotland) Act Assessment Team's review carried out by

A handwritten signature in blue ink that reads "Iida Saarinen". The signature is written in a cursive style.

Iida Saarinen
Public Records Officer



East Lothian Council Data Protection November 2022

Conclusion

Reasonable Assurance

Contents page

Executive Summary	3
Headlines	4
Areas where expected controls are met/good practice	5
Detailed Recommendations	6
Appendices	
Appendix A – Recommendation Grading/Overall opinion definitions	11
Appendix B – Resource, acknowledgements & distribution list	12

1 Executive Summary: Data Protection

Conclusion: Reasonable Assurance

The Council has a comprehensive set of policies, procedures and guidance covering Data Protection, together with clearly defined roles and responsibilities which seek to ensure compliance with General Data Protection Regulations (GDPR) and the Data Protection Act 2018. The Council has a Data Protection Policy in place, which was approved by Cabinet on 12 June 2018, and the Information Governance section of the Council’s intranet provides employees with a wide range of documentation on Data Protection, including the GDPR Toolkit, which contains guidance, templates, training and tools to assist staff to understand and comply with their Data Protection obligations. The Council’s website provides members of the public with details of individuals rights to access their own personal data, including making a “Subject Access Request”. However progress on the development of Information Asset Registers has been slow and staffing challenges within the Information Governance Team have resulted in delays in the implementation of some new processes.

Background

Data Protection is about safeguarding personal and sensitive information and empowering individuals to understand how and why we use their data. On 25 May 2018, the European General Data Protection Regulation (GDPR) came into effect, which in the UK was given effect by the Data Protection Act 2018 (DPA 2018). As of 1 January 2021, this is now underpinned by the UK General Data Protection Regulations (UK GDPR), which are distinct from the EU GDPR.

Summary of findings & recommendations

The following key findings and recommendations are highlighted, which have all been **agreed by the Team Manager – Information Governance and Service Manager – Governance**:

- There is a backlog of Information Sharing Agreements (ISAs) that require to be put in place with organisations with whom personal data is shared. *Management have confirmed that following recruitment of new posts, processes for approving ISAs are to be simplified and streamlined by June 2023*.*
- There has been limited progress on the development of Information Asset Registers for areas in the Council where data processing activities are undertaken. *Management have confirmed that there will be continuous development of the Information Asset Register, with four workshops being held with service areas per annum on an ongoing basis*.*
- The Council has appropriate policies, procedures and guidance documents in place for all aspects of Data Protection, however in some cases these policies and procedures require to be reviewed and updated. *Management have confirmed that these will be reviewed and updated by April 2023.*
- Data Protection risks are recorded and reported as part of both the Corporate Support Risk Register and the Council’s Corporate Risk Register, which detail both control measures currently in place and planned control measures, however there has been slippage to the timescales for implementing some of the planned control measures. *Management have agreed to progress implementation of existing planned risk control measures by June 2023*.*
- Training for all staff on Data Protection is made available via e-learning, online and printed guidance, supplemented by person-to-person training where required, however roll-out of the Communications Plan is required to reinforce the importance of Data Protection compliance. *Management have agreed that the Communications Plan will be rolled-out, with support from IT Infrastructure & Security and Communications Teams by June 2023*.*

Recommendation Summary

Recommendations Grade	High	Medium	Low	Total
Current Report	-	5	-	5
Prior Report	n/a	n/a	n/a	n/a

Materiality

Personal data is defined as any information relating to a person who can be directly or indirectly identified. This includes identifiers including names, identification numbers, location data, online identifiers or any other information that identifies an individual. Special category/sensitive personal data is information which falls under specific definitions under GDPR. This includes racial or ethnic origin; political opinions; religious or philosophical beliefs; genetic data; biometric data; health data; sex/gender or sexual orientation.

*Dates agreed are contingent on capacity within other Council Services.

2 Headlines

Objectives	Conclusion	Comment
1. The Council has clear and appropriate policies, procedures and guidance documents in place for all aspects of Data Protection, together with clearly defined roles and responsibilities.	Reasonable	The Council has a comprehensive set of policies, procedures and guidance in place for Data Protection, although in some cases these require to be reviewed and updated. The Council's intranet contains guidance, templates, training and tools to assist staff to understand and comply with their data protection obligations, while the Council's website provides details of what kinds of personal data we collect and individuals rights to access their own personal data.
2. Appropriate arrangements are in place for the fair collection and use of personal data, through the use of Privacy Notices.	Reasonable	Arrangements are in place to ensure that personal data is processed in accordance with Privacy Notices issued to individuals by the relevant Council service at the point of data collection. Guidance for staff and a standard Privacy Notice template is available on the Council's intranet.
3. Appropriate arrangements are in place for sharing personal data, including Information Sharing Agreements (ISAs) with organisations with whom personal data is shared.	Reasonable	Appropriate arrangements are in place for sharing data, including Information Sharing Agreements (ISAs) with organisations with whom personal data is shared, to ensure that data sharing is in compliance with legislation and the Council's Data Protection Policy, however staffing challenges have resulted in a backlog of ISAs that require to be put in place.
4. The Council is making appropriate progress in the development of an Information Asset Register, to enable compliance with GDPR and the DPA 2018.	Limited	The Council's Data Protection Policy states that a record of data processing activities will be maintained in an Information Asset Register (IAR), which will identify staff members responsible for overseeing compliance with each processing activity (Information Asset Owners), however progress to date has been slow and IARs are not currently in place for many areas of the Council.
5. The Council has appropriate procedures in place for responding to, documenting and, where appropriate, reporting Data Breaches/Near Misses.	Reasonable	Appropriate arrangements are in place for responding to, documenting and, where appropriate, reporting Data Breaches/Near Misses. Guidance is available to employees on the intranet, and a Data Breach Procedure and management procedures for Information Governance staff are both in place. A detailed Data Breach Register is maintained, together with appropriate case files.
6. Arrangements are in place to ensure that risks regarding Data Protection are regularly reported to a senior level, and there is appropriate reporting to Members on Data Protection matters.	Reasonable	Data Protection is a standing item at the Corporate Risk Working Group and risks are recorded on both the Corporate Support Risk Register and the Council's Corporate Risk Register. The Council's Corporate Risk Register, includes a combined risk (ELC CR4) on Information Security and Data Protection. Planned control measures have been identified to reduce the current risk, and while there has been slippage to the timescales for implementing some of these control measures, there has been ongoing progress on the DSA process review and the new DPIA forms.
7. Appropriate Data Protection training is made available to staff via e-learning, online and printed guidance.	Reasonable	Data Protection training is made available to staff via e-learning, online and printed guidance, supplemented by person-to-person training where required, and work is ongoing on developing a Communications Plan to reinforce awareness of Data Protection across the Council.
8. Appropriate Data Protection consideration and input has been provided as part of the response to the Covid-19 pandemic.	Reasonable	The Information Governance Team were heavily involved in Data Protection aspects of the Council's response to the Covid-19 pandemic, including advising Connected Communities, ensuring that volunteers understood their Data Protection obligations, preparing a Test and Protect attendance sheet and developing a Privacy Notice Covid-19 contact tracing template.

3 Areas where expected controls are met/good practice

No	Areas of Positive Assurance
1.	<p>The Council has a Data Protection Policy in place, which was approved by Cabinet on 12 June 2018, and includes the following:</p> <ul style="list-style-type: none">• Definitions of personal data, special category data, records, processing, Data Controller (the Council), Data Processor and Data Subject.• Key roles and responsibilities – including the Senior Information Risk Owner (Head of Corporate Support) and the Data Protection Officer (DPO). The DPO is a statutory role under GDPR and the Council’s DPO is the Team Manager – Information Governance.• The Data Protection principles and how the Council will ensure compliance with the principles.• The rights of individuals regarding their personal information.• Processes for information handling, collection, security, records management, complaints, enforcement and dealing with breaches.• Details of related policies and procedures, including GDPR Toolkit, Data Breach Procedure, IT Acceptable Use Policy, Information and Records Management Policy and ELC Retention Schedule.
2.	<p>The Information Governance section of the Council’s intranet provides employees with a wide range of documentation on Data Protection, including the GDPR Toolkit, which contains guidance, templates, training and tools to assist staff to understand and comply with their Data Protection obligations. The Access to Information section of the Council’s website provides members of the public with information on Data Protection, including Our Privacy promise; What kinds of personal data do we collect; How do we collect your personal data; and How do we use your personal data. The website provides details of individuals rights to access their own personal data, including making a “Subject Access Request” and provides a link to the Information Commissioner’s website.</p>
3.	<p>Individuals have new and enhanced rights under GDPR, including the right to request the erasure of their personal information, the right to restrict processing of their data, the right to data portability, and the enhanced right to be informed about how their information will be used. The Council has appropriate documentation, processes and templates in place for recording and responding to requests received from individuals, including Subject Access Requests and Individual Rights Requests.</p>

4 Detailed Recommendations

Policies, Procedures and Guidance

Objective 1	Finding & Risk 1	Grade	Recommendation
	<p>We sought to ensure that the Council has clear and appropriate policies, procedures and guidance documents in place for all aspects of Data Protection, together with clearly defined roles and responsibilities. The Council has a Data Protection Policy in place, which was approved by Cabinet on 12 June 2018, and includes the following:</p> <ul style="list-style-type: none"> • Definitions of personal data, special category data, records, processing, Data Controller (the Council), Data Processor and Data Subject. • Key roles and responsibilities – including the Senior Information Risk Owner (Head of Corporate Support) and the Data Protection Officer (DPO). The DPO is a statutory role under GDPR and the Council’s DPO is the Team Manager – Information Governance. • The Data Protection principles and how the Council will ensure compliance with the principles. • The rights of individuals regarding their personal information. • Processes for information handling, collection, security, records management, complaints, enforcement and dealing with breaches. • Details of related policies and procedures, including the GDPR Toolkit, Data Breach Procedure, IT Acceptable Use Policy, Information and Records Management Policy and ELC Retention Schedule. <p>The Information Governance section of the Council’s intranet provides employees with a wide range of documentation on Data Protection, including the GDPR Toolkit, which contains guidance, templates, training and tools to assist staff to understand and comply with their Data Protection obligations. The Access to Information section of the Council’s website provides members of the public with information on Data Protection, including Our Privacy promise; What kinds of personal data do we collect, How do we collect your personal data; and How do we use your personal data. The website provides details of individuals rights to access their own personal data, including making a “Subject Access Request” and provides a link to the Information Commissioner’s website.</p> <p>In summary, the Council has a comprehensive set of policies, procedures and guidance, however in some cases we found that these require to be updated, including for example the Records Management Plan which is for the period 2014-2019 (although we note that an action plan is in place in line with previous audit recommendations, which was reported to Cabinet in March 2022) and the IT Acceptable Use Policy, for which the version that is currently available on the Council’s intranet was last updated in July 2015.</p>	Medium	<p>1.1 Management should seek to ensure that relevant policies and procedures are reviewed and updated on a regular basis.</p>

Management response	Responsible officer & target date
<p>1.1 Agreed – relevant policies, procedures and guidance will be reviewed and updated, in conjunction with colleagues in other areas of the Council.</p>	<p>Team Manager – Information Governance April 2023</p>

4 Detailed Recommendations

Information Sharing Agreements

Objective 3	Finding & Risk 1	Grade	Recommendation
	<p>We sought to ensure that appropriate arrangements are in place for sharing data, including Information Sharing Agreements being in place with organisations with whom personal data is shared. The Council’s Data Protection Policy (Section 14.3) states that “in order to improve service delivery and to meet its responsibilities, the Council may enter into data sharing agreements with other organisations where data sharing is allowed by law. Where this is the case, the Council will ensure that an Information Sharing Agreement with that organisation is in place which ensures that data sharing is in compliance with the law and this policy”.</p> <p>The Information Governance section of the Council’s intranet contains a section on Sharing Personal Data, which includes a detailed Information Sharing Agreement template. In addition, the Information Governance Team have a number of other documents, including a:</p> <ul style="list-style-type: none"> • Data Sharing Agreement (DSA) Approval Procedure; • DSA Approval Process Diagram; • DSA Approval Request Form – Email Template; • DSA Assessment Checklist; and • DSA Assessment Checklist Guidance. <p>The DSA Approval Process Diagram clearly outlines the process in place, which starts with a service user request to the IT Service Desk, the service user is asked to complete the DSA Approval Request Form, it is then allocated to the Information Governance Team who create a case file, pass it to the Information Security Team for review, undertake appropriate assessments and reviews (with internal sign-off) and discuss the DSA with the service user and supplier/external organisation. The DSA is then sent to the supplier/external organisation for signature and on return is signed on behalf of the Council, stored and updated on the Data Sharing Register.</p> <p>As part of the audit, we reviewed the Data Sharing Register and found that it records the reference, Title/Organisation the DSA is with, the owning service area, the data received, the date of response and the Data Protection Impact Assessment (DPIA) if appropriate. We note however that staffing challenges within the Information Governance Team have resulted in there currently being a backlog of Information Sharing Agreements that require to be put in place.</p>	Medium	3.1 Management should ensure that Information Sharing Agreements are put in place on a timely basis.

Management response	Responsible officer & target date
<p>3.1 Agreed – the processes for approving Information Sharing Agreements are being simplified and streamlined. Full roll-out of the new processes to be completed following recruitment of the new Team Leader – Information Governance.</p>	<p>Team Manager – Information Governance June 2023 contingent on capacity within other Council Services.</p>

4 Detailed Recommendations

Information Asset Register

Objective 4	Finding & Risk 1	Grade	Recommendation
<p>The Council's Data Protection Policy (Section 12.3) states that a record of data processing activities will be maintained by the Council in an Information Asset Register, which will identify the members of staff responsible for overseeing compliance with each processing activity (Information Asset Owners).</p> <p>The Information Governance section of the Council's intranet contains a section on Information Asset Registers, which includes details of:</p> <ul style="list-style-type: none"> • An Information Asset Register (IAR) template. • How to fill out the Information Asset Register. • Example Workflows. • Beginners Guide to Information Asset Registers. <p>An Information Asset is defined by the National Archives as "a body of information defined and managed as a single unit". Information Assets are defined by the activity that produces them, not by the system that stores them. The Beginners Guide to Information Asset Registers defines an IAR as "a mechanism for understanding and managing an organisation's information assets and the risks to them, including the links between the information assets, their business requirements and technical dependencies". An important part of developing an IAR is identifying information flows from the point information enters the Council, through internal management and out to both internal and external stakeholders. There are some minimum requirements for an IAR, as defined by the UK Information Commissioners Office (ICO):</p> <ul style="list-style-type: none"> • Is there an identified owner for the IAR itself? • Is the IAR regularly reviewed and updated? • Is the IAR linked to corporate retention schedules and risk registers? <p>The Beginners Guide to Information Asset Registers further states that an Information Asset Owner (IAO) is responsible for ensuring that the information is managed appropriately, and at ELC, IAOs should be designated at Service Manager level or above. The Guide further states that ELC is currently developing an IAR and is beginning to collect basic information to enable compliance with GDPR and the Data Protection Act 2018. As a first step, IAOs are asked to complete a spreadsheet regarding their information assets, which should assist in the recording and managing of information assets consistently across the Council.</p> <p>We note that the Council has detailed retention schedules in place as part of Records Management processes, however progress in respect of the IARs has been slow. IARs are in place for the Feedback Team and for Public Protection, but IARs are not currently being maintained for other areas within the Council which undertake data processing activities.</p>		Medium	4.1. Management should ensure that appropriate progress is being made in the development of Information Asset Registers for all areas in the Council where data processing activities are undertaken.
Management response		Responsible officer & target date	
4.1 Agreed – there will be continuous development of the Information Asset Register, with four workshops being held with service areas per annum.		Team Manager – Information Governance Ongoing	

4 Detailed Recommendations

Reporting of Risks

Objective 6	Finding & Risk 1	Grade	Recommendation
	<p>We sought to ensure that information regarding Data Protection is regularly reported at a senior level, and that there is appropriate reporting to Members on Data Protection matters. Data Protection is a standing item at the Corporate Risk Working Group and risks are recorded on both the Corporate Support Risk Register and the Council’s Corporate Risk Register, which are both reported to the Audit and Governance Committee on an annual basis. In particular we note that:</p> <ul style="list-style-type: none"> • The Corporate Support Risk Register (as at September 2022) has a dedicated risk covering Data Breaches/Compliance which highlights the risk of breaches of personal data through accidental disclosure or loss of data in transmission, lack of staff awareness, intentional or malicious misuse of personal data and lack of appropriate provisions for storage or disposal of personal data. The Corporate Support Risk Register identifies risk control measures currently in place, and planned control measures, which when implemented will reduce the risk from High to Medium. Target dates of implementation are identified for each of the planned risk control measures. • The Council’s Corporate Risk Register was presented to Council in March 2022 and to the Audit and Governance Committee in June 2022, although it is updated on an ongoing basis. The most recent version of the Risk Register (September 2022) includes a combined risk (ELC CR4) on Information Security and Data Protection. The assessment of current risk is Very High, although this is primarily due to the elevated risk of external information security threats due to global events, rather than governance controls. In respect of Data Protection, the risk highlights the consequences of breaches of the Data Protection Act 2018/GDPR, emphasises the importance of good records management and the most recent Risk Register reported (June 2022) noted that Subject Access Requests have increased both in number and complexity and that with FOI requests also increasing, combined with staffing challenges, there was a higher risk of missing statutory response timescales. A number of planned risk control measures have been identified covering Training and Awareness, Information Transformation Strategy, Records Management Plan, DSA/DSIA Process Reviews, and Dunbar Road Options Paper. The assessment of current risk (with the proposed planned control measures) is reduced from Very High to High. We note however that there has been slippage to the timescales for implementing some of these control measures, between the June 2022 and September 2022 versions of the Corporate Risk Register, in particular the timescale for the Training and Awareness Communications Plan has moved from June 2022 to January 2023 and the timescale for completion of DSA/DPIA Process Reviews has moved from December 2022 to April 2023. We are advised however that although completion dates have extended there has been ongoing progress, for example the DSA process review is complete with new procedures in place and training delivered to the team, while there is a new rapid DPIA form which is now in use and a completed draft of a new long form. 	<p>Medium</p>	<p>6.1 Management should ensure that timescales for planned risk control measures are realistic and are implemented on a timely basis.</p>
<p>Management response</p>		<p>Responsible officer & target date</p>	
<p>6.1 Agreed – implementation of existing planned control measures will be progressed. Full roll-out of all planned risk control measures following recruitment of the new Team Leader – Information Governance.</p>		<p>Team Manager – Information Governance June 2023 contingent on capacity within other Council Services.</p>	

4 Detailed Recommendations

Training

Objective 7	Finding & Risk 1	Grade	Recommendation
<p>The Council’s Data Protection Policy (section 1.3) states “the Council is fully committed to data protection compliance and will follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, volunteers and any other partners of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and comply with their duties and responsibilities under GDPR and the Data Protection Act 2018”. The Policy further states:</p> <ul style="list-style-type: none"> • Individual members of staff and elected members are responsible for protecting personal information held or processed on computer, or held in paper records, within their care. • Heads of Service and Service Managers will ensure that all staff have access to the Data Protection Policy and that they receive relevant training. • Training for all staff will be made available via e-learning, online and printed guidance, supplemented by person-to-person training where required. <p>Data Protection awareness training is a mandatory part of induction and must be refreshed every two years. The Council’s intranet pages for Information Governance also include templates, guidance and information to support corporate compliance. Training is refreshed and reviewed on a regular basis and includes:</p> <ul style="list-style-type: none"> • The module content for the mandatory e-learning module on Data Protection, which was refreshed and redesigned in May 2022. • The Council’s intranet contains “GDPR Training: offline training” which can be provided to those individuals who do not have access to the e-learning module, together with guidance on “Data Protection Principles” and “Data Protection Do’s and Don’ts”. <p>As part of our review it was identified that 2,981 (58%) out of 5,158 LearnPro users were up to date with their mandatory Data Protection module. This indicates that there is scope for improvement in the uptake of this module and we note that line managers have access to the LearnPro scorecard to enable them to check who in their team has completed the training. Key risks to the Council in respect of data breaches/compliance have been identified as lack of staff awareness and the accidental disclosure or loss of personal data in transmission. The Team Manager – Information Governance, Team Manager – IT Infrastructure & Security and Communications Teams are progressing a Communications Plan, including Inform briefings, email updates and other training and briefings to reinforce awareness of data protection and information security across the Council. There has been slippage in the proposed timescales and we are advised that the ability to undertake this work is currently limited by capacity within the Information Governance Team.</p>		Medium	7.1 Management should seek to progress the roll-out of the Communications Plan across the Council to reinforce the importance of Data Protection compliance.
Management response		Responsible officer & target date	
7.1 Agreed – the Communications Plan will be rolled-out, with support from IT Infrastructure & Security and Communications Teams.		Team Manager – Information Governance June 2023 contingent on capacity within other Council Services.	

A Recommendation Grading/Overall opinion definitions

Recommendation	Definition
High	Recommendations relating to factors fundamental to the success of the control objectives of the system. The weaknesses may give rise to significant financial loss/misstatement or failure of business processes.
Medium	Recommendations which will improve the efficiency and effectiveness of the existing controls.
Low	Recommendations concerning minor issues that are not critical, but which may prevent attainment of best practice and/or operational efficiency.

Levels of Assurance	Definition
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

B Resource, acknowledgements & distribution list

Internal Audit	
Service Manager, Internal Audit: Duncan Stainbank	Senior Auditor: Stuart Allan

Review Dates	Completed By Date
Internal Audit Draft Report Submission	07 November 2022
Management Review Completion	17 November 2022
Final Report Issue	23 November 2022

Report Distribution	
Chief Executive	Executive Director for Council Resources
Head of Corporate Support	Service Manager – Governance
Team Manager – Information Governance	External Audit

Acknowledgements:

The weaknesses identified during the course of our audit have been brought to the attention of Management. The weaknesses outlined are those, which have come to our attention during the course of our normal audit work and are not necessarily all of the weaknesses, which may exist.

Although we include a number of specific recommendations, it is the responsibility of Management to determine the extent of the internal control systems appropriate to Data Protection.

The contents of this report have been discussed with the Team Manager – Information Governance and Service Manager – Governance. The assistance and cooperation received during the course of our audit is gratefully acknowledged.



PO Box 29105, London
SW1V 1ZU

Ms. Monica Patterson
Chief Executive
East Lothian Council
John Muir House
Haddington
EH41 3HA

chiefexec@eastlothian.gov.uk

8 March 2022

Dear Chief Executive,

IPCO CHIS and Surveillance Inspection of East Lothian Council

Please be aware that IPCO is not a “public authority” for the purpose of the Freedom of Information (Scotland) Act (FOISA) and therefore falls outside the reach of the FOISA. It is appreciated that local authorities are subject to the FOISA and that they may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the attention of the IPCO Data Protection Officer (at: info@ipco.org.uk), before making any disclosure. This is also the case if you wish to make the content of this letter publicly available.

Your authority was recently subject to a remote inspection by one of my Inspectors, Mr. Paul Donaldson. The documentation and arrangements necessary for my Inspector to carry out the process was provided by Ms. Zarya Rathe, Team Manager, Information Governance and Data Protection Officer, who now acts as your RIPSAs Coordinator/Gatekeeper. This enabled an examination of relevant policies, ten directed surveillance authorisations granted since the last inspection in January 2019, along with two applications which had been refused by your Authorising Officer (AO). Ms. Rathe, along with Ms. Morag Ferguson, Head of Corporate Support, who is relatively new to the role of Senior Responsible Officer (SRO), and Mr. Carlo Grilli, Head of Governance, made themselves available to be interviewed via video conferencing. From the documentation examined and the information provided during the interview, the level of compliance shown by your authority removes, for the present, the requirement for a physical inspection.

At the last inspection your authority was subject to five recommendations, and I note there being a comprehensive action tracker developed to monitor progress in addressing those. In terms of Recommendation 1, my Inspector is satisfied the practice of backdating cancellations no longer exists and can be discharged. Recommendation 2 related to reporting RIPSAs matters to Elected Members, and I note that the initial plan to institute this practice was placed on hold due to the pandemic. I understand that a new process to ensure Elected Members are briefed on RIPSAs issues as per paragraphs 4.43¹ and 3.27² will be introduced once the new committee structure is established after the upcoming local government elections. In view of these matters, Recommendation 2 will remain extant until the process is embedded.

¹ Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017

² Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

Recommendation 3 related to AOs stipulating incorrect duration periods within directed surveillance authorisations. I note from the observations outlined below by my Inspector that this practice was still evident, and therefore this recommendation will also remain extant. I appreciate that the nominated AOs within the Council have also changed recently and that there is a plan in place to deliver appropriate training to them, to ensure they are fully aware of their RIPSAs responsibilities. It is worth highlighting that your RIPSAs Coordinator has developed very useful *Guidance for Authorising Officers* documents which cover the key elements within the authorisation process very well.

Recommendation 4 suggested a review of the practice of authorising directed surveillance under RIPSAs for monitoring noise levels where anti-social behaviour complaints were made. Where it is decibel levels being recorded, there is little chance of any private information being obtained and I note that, whilst no longer a widespread practice, one such authorisation was granted (2019/004). This was discussed with current staff, who have a clear understanding of the guidance and the recommendation is therefore discharged. I understand situations can arise where the full capability of the equipment may not be understood, and a doubt may exist as to whether voices are being recorded. Where such uncertainty does exist, it is essential that AOs understand the full capabilities of the equipment, to assess the necessity of authorising its deployment as directed surveillance. For ease of reference, paragraph 3.37³ provides some additional guidance on the matter.

Recommendation 5 outlined adjustments to be made to your policies, and my Inspector has intimated that those have been made and that the RIPSAs policy and the accompanying appendices covering the use of CHIS and covert surveillance, including the *Surveillance through Social Media Policy*, are currently being reviewed further. I am aware that he has offered specific guidance in respect of the contents of each of the policies mentioned, in particular the guidance offered in section 8 (*Utilisation of Social Media*) of the *Surveillance through Social Media Policy*. I direct you to the contents of paragraphs 3.5 to 3.7⁴, 3.11 to 3.16⁵, and 4.7 to 4.14⁶ and of the need for your guidance to reflect the principles contained within these sections.

The use of the internet and social media is a valuable investigative resource and oversight and auditing of its use is critical within all public authorities, whether authorised under RIPSAs or not. In that regard my Inspector discussed The Investigatory Powers Tribunal's (IPT) decision in *BA & others v Chief Constable of Cleveland IPT/11/129/CH (13 July 2012)*, where the IPT commended the adoption in non-RIPAs (RIPSAs) cases "a procedure as close as possible" to that required by the legislation. Records being maintained of online activity in investigations allows for appropriate auditing and serves to reduce the risk of there being any disproportionate use of social media. I note that there is an intention when further training is delivered, for there to be relevant content included to ensure these principles can be introduced.

Mr. Donaldson examined ten directed surveillance authorisations granted since the last inspection, and two rejected applications, and makes the following points:

1. The applicants provided sufficient and specific background information on investigations to enable the requisite elements of necessity, proportionality, and collateral intrusion to be considered, as per paragraph 5.4⁷.
2. Whilst the relevant content is present, it seems applicants at times conflate considerations of necessity and proportionality. Applicants should focus on the elements contained within paragraph 4.7⁸.

³ Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

⁴ Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017

⁵ Ibid

⁶ Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

⁷ Ibid

⁸ Ibid

3. There were insufficient considerations attached to collateral intrusion by the applicants and AOs where the deployment of covert cameras had been authorised. It is essential that there is a clear understanding of the capabilities of the equipment, the impact on collateral intrusion, or how the risks can be controlled and managed (2019/003).
4. AOs continue to set expiry dates which do not comply with the legislation, i.e. a duration of three months. AOs can set review dates to allow them to assess the continued necessity and proportionality of the authorised activity as per paragraph 8.11⁹, but cannot shorten the authorisation period.
5. AOs should ensure their authorisations are maintained in accordance with paragraphs 5.19 to 5.21¹⁰ and Chapter 8 of the Code of Practice. Cancellations should provide detail on what activity has been undertaken, the type and extent of the product and material obtained, and how it is to be managed, with the AO providing some direction or instruction for its management.

Mr. Donaldson has highlighted that the new SRO and RIPSAs Coordinator are in the process of developing a programme of training which will include an input from an external provider, as well as the introduction of an e-learning module to be made available to all staff. I view the provision of training and availability of RIPSAs awareness material as being critical to ensuring that staff are suitably equipped should they contemplate covert activity in the course of their investigations. I was also pleased to learn that the RIPSAs Coordinator intends to introduce a quality assurance process where applications and authorisations will be reviewed prior to submission to the AO and to offer guidance where appropriate.

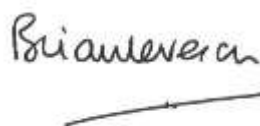
I am aware that since the last inspection you have received my letter outlining IPCO's recent Data Assurance Programme and that you have in place an *Information and Records Management Policy*, as well as a *Business Classification Scheme and Retention Schedule*. Whilst these policies cater for material obtained from CCTV, they do not explicitly cater for material collected through the use of covert powers under RIPSAs. It was highlighted that this is being addressed as part of the review of the relevant policies, and I would encourage you to ensure the guidance is aligned with the content of the relevant Codes of Practice and with the principles outlined in my aforementioned letter.

I am conscious of the period of change within your Council in respect of those who occupy the roles associated to RIPSAs governance, and within time the revised policies and processes will be established. On the whole, I am satisfied that there is a clear direction of travel to maintain compliance with the legislation and Codes of Practice and I would highlight that the observations made herein will assist your staff in their respective roles should they need to utilise covert investigative techniques.

I hope that you find the outcome of this remote inspection helpful and constructive, and my Office is available should you have any queries following the receipt of this letter, or at any point in the future. Contact details are provided below. I shall in any case, be very interested to learn of your proposed response to the observations made within this letter, and of the progress being made, within the next two months.

The Inspector would like to thank your staff for their very positive engagement and transparency throughout this remote inspection process, and for providing the necessary documentation to enable it to be achieved.

Yours sincerely,



The Rt. Hon. Sir Brian Leveson
The Investigatory Powers Commissioner

⁹ Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

¹⁰ Ibid