Information Governance Annual Report 2024/25

Version 3.0

2025

Document Control Sheet

Date of Creation:	September 2025
Owner (Service):	Information Governance Manager & DPO
Reviewer Head of Service:	Chief Governance Officer (Monitoring Officer)
Approver Executive Director:	Executive Director for Economy, Enterprise and Operations
Date Approved:	
Approver (Committee):	Corporate Committee
Date Approved:	
Next Review Date:	

Version History

Version	Date	Author	Changes Made	Approved By
1.0	**Nov 2023**	Information Governance Manager & DPO	Initial document for 2022/23	Corporate Committee
2.0	**Aug 2024**	Information Governance Manager & DPO	Updated for 2023/24	Corporate Committee
3.0	**Sept 2025**	Information Governance Manager & DPO	Updated for 2024/25	

Contents

1. Introduction

Information Governance (IG) is an umbrella term that covers anything the Council does with information; ensuring appropriate governance and processing of the Council's information is an ongoing activity.

IG policies and guidance documents are set out in Appendix A and acronyms in Appendix B.

2. Access to Information

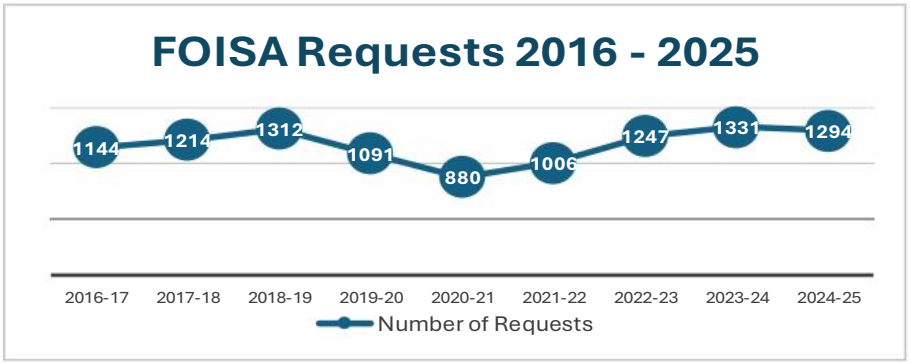
2.1 FOISA and EIR - Information Requests

The Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EIR) give anyone the right to request recorded information held by the Council, subject to certain exemptions. All information held regardless of whether the Council created or received it, and, regardless of format, is subject to such requests.

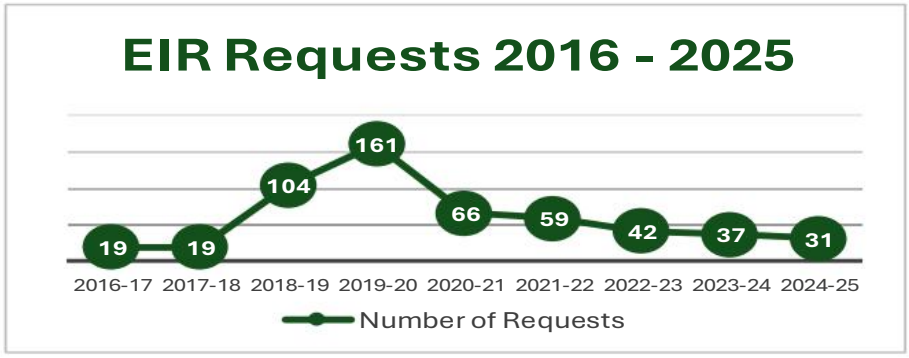
All FOISA and EIR requests for information held by the Council or Moray Integration Joint Board (MIJB) are logged, co-ordinated, collated and responded to by the FOI Team (Information Co-ordinator). The Council must respond to any request received within 20 working days.

The Scottish Information Commissioner (SIC) enforces and promotes FOISA and EIRS as an independent public official. The SIC is responsible for dealing with complaints and promoting good practice, and, collects and publishes quarterly FOISA and EIR statistics.

FOISA and EIR Information Requests 2016 – 2025



- In comparison to 2023/24, the Council received 37 fewer FOISA Requests.



- In comparison to 2023/24, the Council received 6 fewer EIR requests.

2.2 FOISA and EIR - Internal Reviews

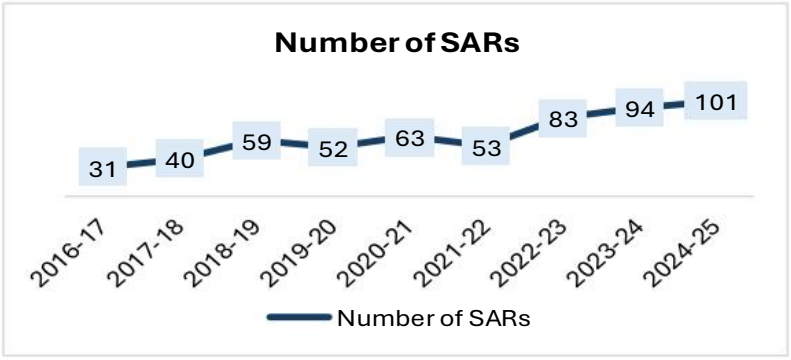
If the Requester is dissatisfied with the Council's response, including a lack of response within the timescales, then the Requester can ask the Council to review its response. Legislative timescales again apply and if the Requester is still dissatisfied then they have the right to appeal

to the SIC. The SIC can order the Council to disclose some or all of the requested information should the SIC determine information was incorrectly withheld. An SIC notice is legally binding; any appeal lodged is heard by the Court of Session.

In comparison to 2023/24, the Council received 3 more FOI Review Requests.

2.3 Data Protection Rights Requests

Data protection law gives people (data subjects) the right to make a "Subject Access Request (SAR)" to access their personal data, which must be provided within 1 calendar month. The Information Commissioner's Office (ICO) oversees and enforces data protection rights.



- The number of SARs received continues to increase. SARs are very resource intensive involving a great deal of officer time to collate and redact information.

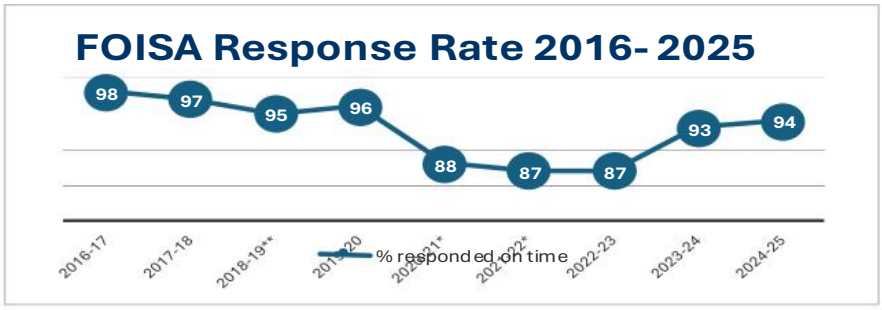
2.4 Access to Information Performance Indicators

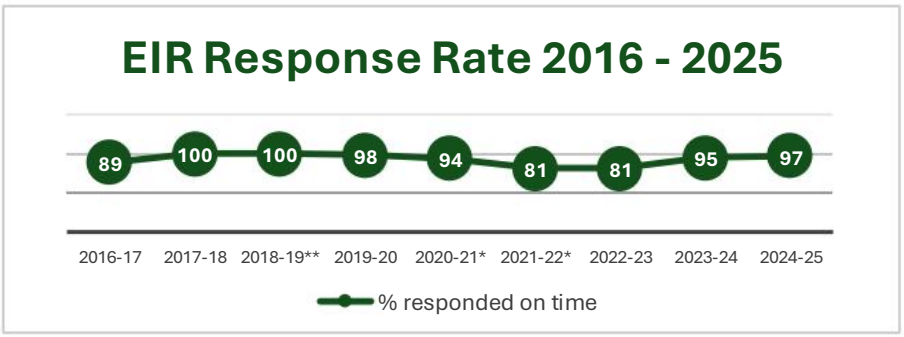
Year	FOI (hrs)	EIR (hrs)	SAR (hrs)	Total (hrs):	Total (days):
2024/25	1492.15	28.8	*350+	1871.00	258.1
2023/24	1262	11.45	370.8	1644.25	226.8

**not all timings have been collated yet due to current resource challenges within the IG Team*
These figures do not include the time spent by the IG Team when logging, advising and responding to requests.

The time taken to complete requests has been recorded since 2023/24.

During 2024/25 at least an extra 30 working days were needed to complete requests.





- Compliance with statutory timescales has increased to 94% (FOISA) and 97% (EIR).

*covid legislation extended timescales for release of information

** DPA 2018 and GDPR from May 2018

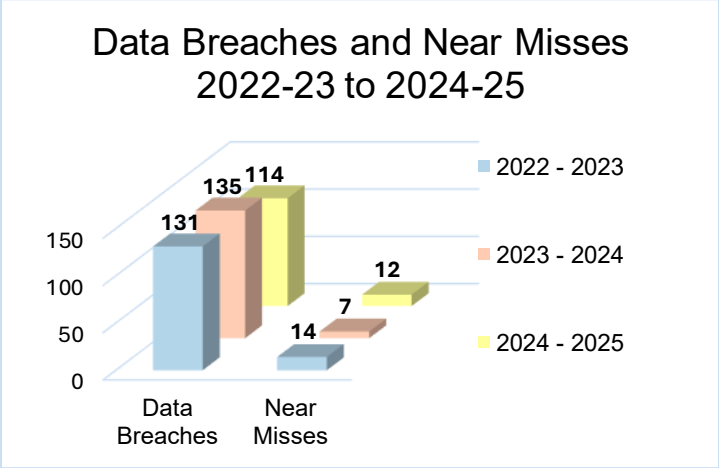
SAR statistics 2024/25

Cases received within date range and responded to:	101	**97% compliance rate**
Cases responded to on time:	98	
Cases responded to that were late:	3	**Please note that of the 3 that were late:** • 2 were negatively impacted by the Council Christmas break. • 1 was negatively impacted by school summer break.
Cases suspended awaiting collection/clarification/ mandate/ID:	22	These cases will have been prompted and/or chased and are just waiting to be closed off when resources allow.
Owing to continued prioritisation and success rates from the IG Team, the ICO only requires annual SAR statistics.		

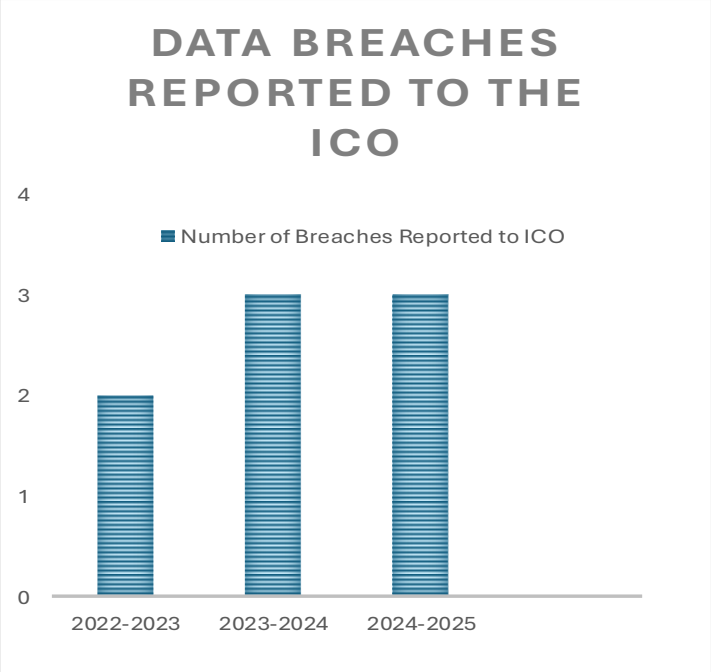
3. Data Protection

3.1 Data Breaches

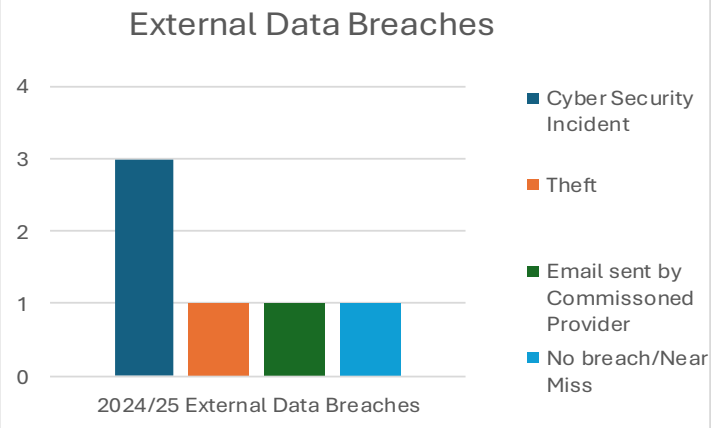
All staff must report data breaches to the Council's Data Protection Officer (DPO) as soon as they are identified or suspected. Breaches present significant reputational and financial risk to the Council. They can cause harm to data subjects, attract complaints or compensation claims, and, result in loss of confidence. Significant breaches must be reported by the DPO to the ICO. The ICO can advise, investigate and even prosecute wrongdoing. The IG Team investigate every report and mitigate against the risk of escalation or reoccurrence.



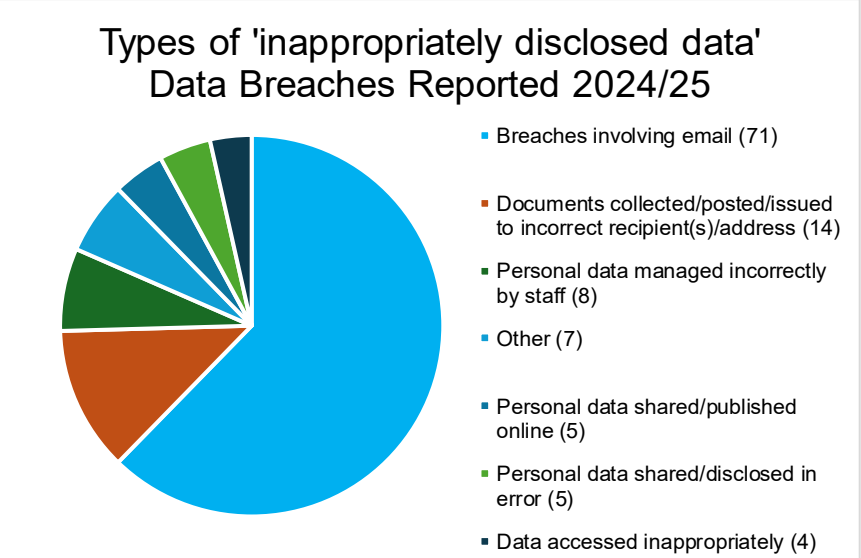
- There has been decrease in the number of reported breaches in comparison to 2022/23 and 2023/24.
- The number of 'near miss breaches' has increased from 2023/24.



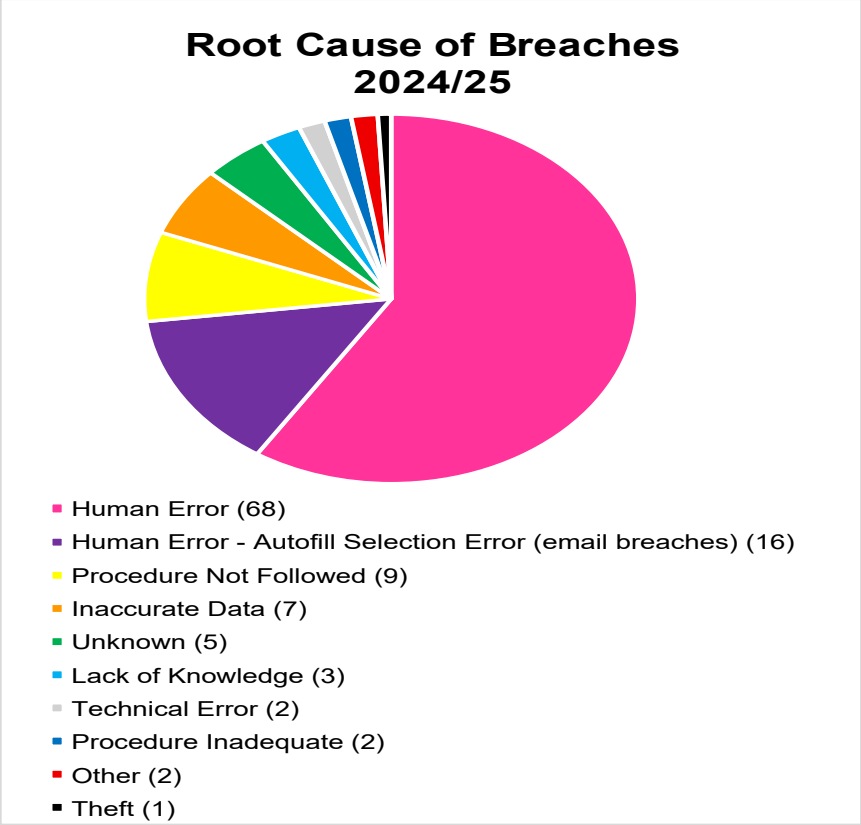
- To date, no penalties attributed and no further action has been taken by the ICO.
- In 2024/25, the three reported breaches related to:
  - Staff member putting a work SIM card into a personal device against guidance directly given to them.
  - Meeting webcast accidentally broadcast after termination of meeting.
  - Personal information shared on Interchange, Service unaware Interchange publicly accessible.



External data breaches are those suffered by third parties holding Council data (processors). There is an increasing risk nationally and internationally of cyber security incidents and much work is ongoing on cyber security. The Council has been recording these incidents since 2024 with a total of 5 recorded for 2024/25.



- The majority of data breaches (101) came from misdirected emails/letters. This continues the trend from 2023/24.



- Where more than one root cause, the breach is recorded against all applicable.
- Human error continues to be the reported root cause of most data breach incidents.
- Each breach is considered on a case-by-case basis and suitable follow up actions are discussed by the IG Team with relevant Services(s).

The IG Team continues to support Services, providing targeted training and support to ensure staff are aware of the set processes to be followed when handling information e.g. how to clear email autofill cache. In addition to maintaining the suite of Data Protection guidance available on the Council's Interchange, the IG Team regularly provide direct advice and guidance.

Baseline controls continue to be in place across the Council, including Data Protection online training available for all staff via CLIVE (LearnPro). Staff are recommended to undertake the Data Protection Refresher training module annually and attend any Service specific Data Protection workshops.

3.2 Information Security

The Council is committed to enhancing cyber security and combating the cyber threats it faces on a regular basis. Cyber security sits within ICT and is monitored on a quarterly basis in the Council's Corporate Risk Register. The IG Team collaborate and work closely with colleagues in ICT to foster a culture of cyber resilience within the Council and reduce the Council's overall exposure to insider/outsider cyber threats.

3.3 Accountability

The Accountability principle requires a proactive approach to data protection; with appropriate measures and records in place to demonstrate compliance. Accountability obligations are ongoing.

The IG Review involving the IG Team reviewing processing activities with Services (commenced in 2022) is ongoing. Progress of this item of work has been slower than hoped as it has been accommodated around ongoing day to day tasks including; access to information requests, management of data breaches, advising on Data Protection Impact Assessments (DPIAs), Data Processing/Sharing Agreements (DPAs/DSAs), privacy notices, management of the Council's closed records stores, and, providing support and guidance to all Services on all aspects of Information Governance.

Number reviewed 2024/2025		
DPIAs	188	• 54 more than in 2023/24 • Internally published DPIA Register
DPAs/DSAs etc	30	• 7 more than in 2024/25
Privacy Notices	41	• Over double the amount updated/created from 2023/24

3.4 Internal Audit – Council's compliance with UK GDPR

Whilst progress has been made there are outstanding and part implemented recommendations (5.01 – 5.07) from Internal Audit's report on the Council's compliance with Data Protection (previously GDPR). Internal Audit have indicated that, whilst there is no current follow up activity being reported through the Audit and Scrutiny Committee it is their intention to revisit this area in future Audit plans. The IG team are prioritising this work with higher risk areas being tackled first

5.01	The Data Protection Policy and guidance should be reviewed to ensure the detailed information remains current and appropriate. Thereafter, a timetable for continued review should be set.

The Data Protection Policy (version 2.0) has been updated and approved Summer 2025. Other guidance is covered in the worklist in Appendix A attached.

5.02	In compliance with UK GDPR, a Record of Processing Activities (ROPA) should be compiled by the Authority based on a data mapping exercise.

and,

5.03	In compliance with UK GDPR, an Information Asset Register (IAR) should also be compiled and maintained on an ongoing basis.

The ROPA, IAR and Appropriate Policy Document (APD) are being reviewed and updated as part of the ongoing IG Review process.

5.04	A review of Privacy Notices held within Council services should be progressed and the documents made available on the Council website for public inspection.

Ongoing action. As each Privacy Notice is updated and composed for revised/new processes they are made publicly available: www.moray.gov.uk/PrivacyNotices.

5.05	Consideration should be given to undertaking reviews within Services to audit compliance with the Data Protection Policy and Guidance. This should provide assurance that the Authority is effectively handling personal data in line with regulations.

Acknowledged as part implemented by Internal Audit. Compliance recommendations are made to Services following data breaches to improve IG practices and reduce the likelihood of a recurrence; also specific IG advice is given upon request and through IG compliance reviews.

5.06	A review of the guidance documents and forms held within the Information Management section of the Interchange should be undertaken and updated accordingly.

The attached worklist of IG policies and guidance at **Appendix A** highlight when document updates and reviews are aimed to be completed. Due to competing priorities the IG Team were unable to meet the original timeframe of March 2025.

5.07	A review should be undertaken of the officers that have not undertaken the data protection training on the LearnPro training system. Any officer identified should be reminded to undertake their data protection training requirement.

In 2024/25, IG Team commenced the development of 'Toolbox Talks' data protection training for non-office-based staff, who do not have access to a computer in their roles. The DP Learnpro module is being refreshed in line with the updated DP Policy, which will then be promoted and uptake will be monitored.

4. Records Management

4.1 Records Management Plan

Under the Public Records (Scotland) Act 2011, Public Authorities must develop and publish a records management plan (RMP) every 5 years. The Council's RMP covers both the Council and Moray Licensing Board, it was last updated and submitted in December 2020. The regulator is the National Records of Scotland (NRS).

The RMP for MIJB is aligned with the Council's RMP. Ten elements (excluding 1, 9, 13, 14 & 15) on MIJB's RMP are directly covered by the Council's RMP. As such the below noted issues will also affect MIJB's RMP.

There are 15 elements to a RMP, with a Red, Amber, Green acceptance scale. The NRS has indicated that:-

GREEN **3 Elements** **(accepted by the Keeper)**	**AMBER** **7 Elements** **(accepted on an 'improvement model' basis)**	**RED** **5 Elements** **(unacceptable)**
1. Identifies Senior Management Responsibility 14. Shared Information i.e. ISAs, ISA Register etc. 15. New element covering public records created by third parties.	2. Identification of the person with Records Management responsibilities. 3. Records and Information Management Policy. 6. Destruction Arrangements. 8. Information Security. 9. Data Protection. DP Policy outdated, limited training and documented and resourcing of DPO role. 11. Audit Trail. 12. Competency framework for records management staff.	4. Business Classification Scheme. 5. Retention Schedules. 7. Archiving and Transfer Arrangements. 10. Business Continuity Plan. 13. Assessment and Review.

The top 3 NRS concerns, with our responses to these are:

1. Level of IG staffing resource - discussed in paragraph 5 below.
2. Lack of progress with a Council wide automated document management system. - Sharepoint was introduced across a number of Council services with the Designing Better Services transformation programme in 2014 but a number of services were not included. This gap has been recognised in the Council's current transformation programme with a wider roll out of M365/SharePoint online. The landscape has also changed with a number of services using information storage systems with built in electronic document management.
3. Archiving provision – discussed in paragraph 4.2 below

Further information is expected from NRS in Autumn 2025. There is a high risk that the Council's RMP is not accepted by the Keeper. If not accepted, then the Keeper will then alert Scottish Ministers, resulting in further action e.g. including a full ICO inspection.

Work is underway to ensure these issues and potential improvements are brought before the Central Leadership Team for consideration of a corporate response.

including working with other services to consider corporate solutions, such as the implementation of M365 as a potential replacement for Shared Drives. The position on the Archives repository and Closed Records Store are being considered through Property Asset Management Review.

4.2 Closed Records Store

The Council's Closed Records Stores (CRS) are required for the secure hardcopy storage of anything the Council must retain for ongoing business or under the Retention Schedules. CRS provision is managed by the IG Team. There are 3 CRS in 3 separate locations within Moray but none conform to the required standards. This has been picked up in the current property review, alongside the Archival storage requirement.

Space for new accessions remains limited and owing to the IG Team's limited resources there is currently a backlog of records awaiting review.

In 2024/25 over 450 new boxes were accessioned into the CRS. Only a quarter of that amount were securely destroyed.

5. Resourcing

Consistent with the 2023/24 report, the Council's IG Team remains resourced at 2.7FTE which is lean when benchmarked against comparable councils.

There has been an increasing trend in the number of time critical information/ subject access requests and review requests. This puts additional pressure on staff time and impacts on time available for records management, policy and development work. This is highlighted as a risk from members to be aware of.

Appendix A – IG Polices and Guidance Documents

Title	Version	Date	Status	Target Date	Notes
Data Protection Policy	v2.0	Aug-25	Up To Date		Update in Spring 2026 with DUAA changes
CCTV Policy	v2.0	Jan-25	Up To Date		Updated for Body Worn Cameras and 'other' cameras, incl. ANPR, dashcams etc
Data Breach Reporting Form	v3.0	Oct-24	Up To Date		
Guidance on Managing Emails	v4.0	Sep-17	Priority 1	30th Sept 2025	Update re:M365, retentions, recall, bulk emails etc
Data Protection Guide	v1.0	Jun-18	Priority 2	Mar 26	To be updated once Policy approved: Update Section 10. Add new AI section and personal devices section.
Information Management: WhatsApp messaging service		Mar-20	Priority 2	June 26	Incorporate into WhatsApp (etc) Policy
Guidance on Data Security Breach Management	v3.0	May-18	Priority 3	Aug 26	Refresh after DP Policy updated
Your Personal Rights Document			Priority 3	Mar 27	
Guidance on Sharing Constituent Information with Elected Representatives (Councillors)	v1.0	Jun-22	Priority 4	Mar 28	
Records Management Reference Handbook		2013	Priority 4	Sept 28	
Subject Access Request (SAR) Procedure	v1.1	Jan-20	Priority 4	Mar 29	Add in a note re - different types of requests e.g. a Spec of Docs?
A Guide to the Freedom of Information (Scotland) Act 2002 (FOISA)	v3.0	Jan-17	Priority 5	Mar 29	Awaiting the revised legislation to go through
A guide to the Environmental Information (Scotland) Regulations, 2004, (EISR)	v1.0	Jan-17	Priority 5	Mar 29	

A Guide to Pupils' Educational Records	v1.0	Mar-17	Priority 5	Mar 29	Update to cite DPA 2018/ UK GDPR
Appropriate Policy Document	v0.4	Feb-23	Priority 5	Sept 29	Current draft to be updated to include CCTV processing.
MIJB Appropriate Policy Document			Priority 5	Mar 30	Council APD as template
Governance and Management of the Closed Record Store (CRS)	v3.0	Sep-23	Priority 5	Mar 30	
Guide on the Identification and Disposal of Confidential Waste	v2.1	May-19	Priority 5	Sept 30	

Appendix B – Information Governance Acronyms

Acronym	Definition
APD	Appropriate Policy Document
CRS	Closed Records Store (CRS).
DPA/DSA	Data Processing Agreement / Data Sharing Agreement
DPIA	Data Protection Impact Assessment. Process designed to assist with systematically analysing, identifying and minimising the data protection risks of a project or plan.
DPO	Data Protection Officer. UK GDPR introduced a duty on public authorities to appoint a DPO. DPOs assist with monitoring internal compliance with Data Protection legislation, informing and advising on Data Protection obligations and reviewing/approving DPIAs. They act as a contact point for data subjects and the Information Commissioner's Office. DPOs must be independent, experts in Data Protection, adequately resourced and report to the highest management level.
FOI	Freedom of Information.
IAR	Information Asset Register.
ICO	Information Commissioner's Office (ICO); independent supervisory authority for data protection in the UK.
RMP	Records Management Plan.
ROPA	Record of Processing Activities.
SAR	Subject Access Request.
SIC	Scottish Information Commissioner.
UK GDPR	United Kingdom General Data Protection Regulation.