Information Governance Management

Annual Report 2025

Senior Information Risk Owner

April 2024 - March 2025

1 Introduction

1.1 The Council's Audit, Risk and Scrutiny Committee agreed the Council's revised and updated Information Governance Management & Reporting Framework in September 2016; as part of this the Committee agreed to receive an annual report in relation to the Council's information governance assurance.

1.2 This report collates, analyses and monitors the Council's performance in relation to freedom of information, data protection and information security, to give assurance that trends, issues, incidents, and breaches are dealt with appropriately as they arise.

1.3 Ensuring the proper use and governance of the Council's information and data is an ongoing activity. New and changing legislation, systems, staff, and ways of doing business, as well as new and emerging cyber threats, all shape and change the environment within which the Council operates in relation to effective use and governance of its information and data.

1.4 Keeping up means a careful balancing between the requirement to monitor and be adaptable to our changing environment, and the requirement to agree and implement assurance improvements over the medium term.

1.5 To this end, actions to improve assurance in the medium term are identified, actioned and monitored through the Information Governance risks on the Cluster Risk Register and the Cyber Security risks on the Corporate Risk Register; regular updates on which are reported separately to the Council's Communities, Housing and Public Protection and Audit, Risk & Scrutiny Committees.

1.6 The Council's Data Protection arrangements were subject to Internal Audit, reported in November 2023. The object of the audit was to provide an assurance review that the Council has adequate controls in place to mitigate the risks identified in the Cluster Risk Register and that these controls are operating as expected. The Audit found a sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied. The level of risk assessed was minor with the control framework deemed to provide substantial assurance over the Council's approach to Data Protection.

1.7 The National Records of Scotland, Public Records (Scotland) Act (PRSA) 2011 Assessment Team, assessed the Council's annual update of its arrangements under the Act in May 2020. The Assessment Team found that the Council continues to take its statutory obligations seriously and maintains the required records management arrangements in full compliance with the Act.

2. Information Governance Performance Information April 2024 - March 2025

2.1 Data Protection Rights Requests

Fig 1: Annual number of requests received

Type of Request	2023/24	2024/25
Subject Access	316	401
Third Party	569	1417
Other Rights Request	27	26

Data Protection Rights Requests

Data protection law gives people certain rights about their data, including the right to access their data.

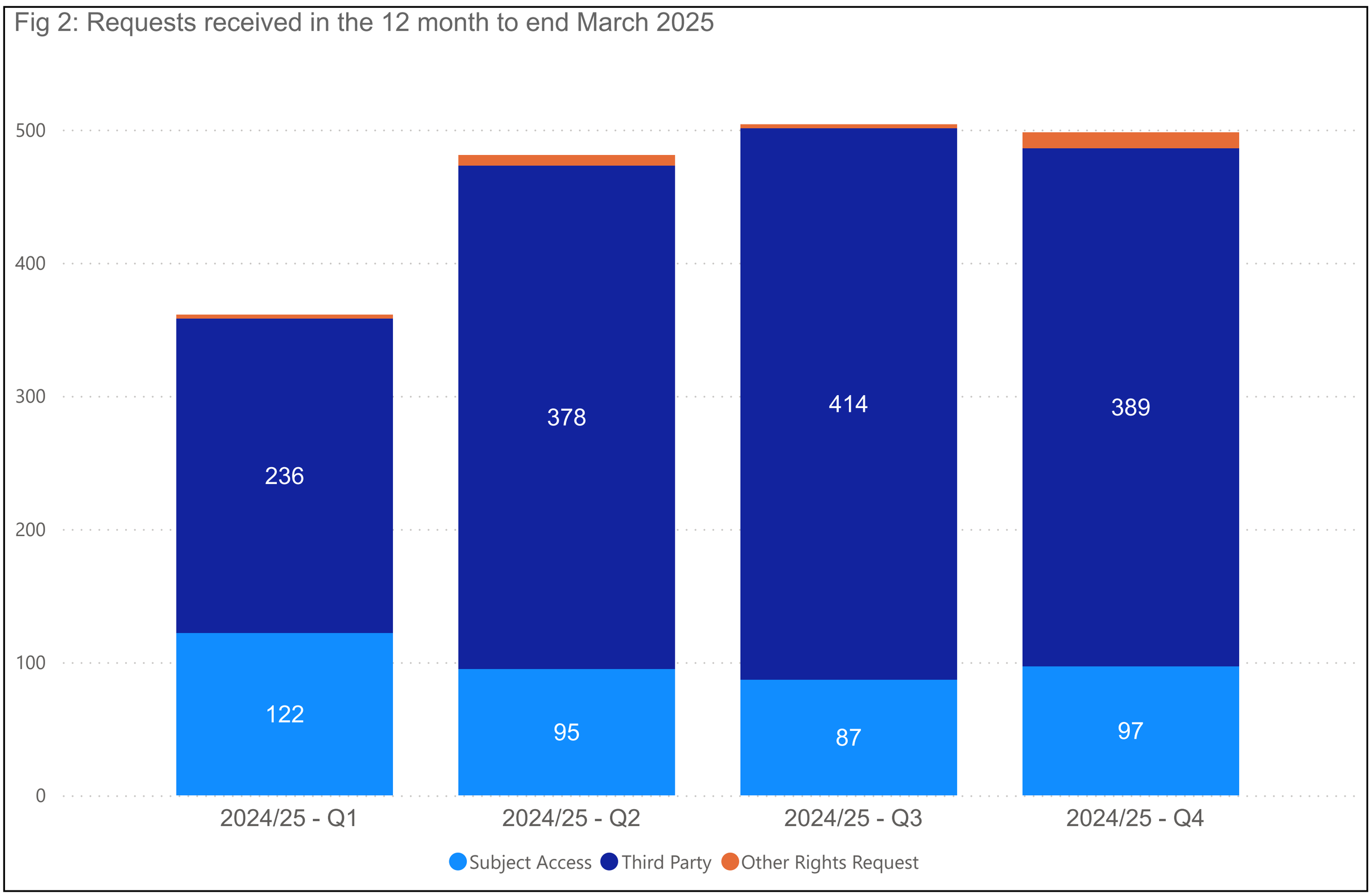
Third Party Requests

Other organisations (for example, Police Scotland, or the Care Inspectorate) can also request a customer's personal data under certain circumstances.

Other Rights Requests

In certain circumstances individuals have other rights around their data: including the right to object, to erasure, to restrict processing and to data portability.

Fig 2: Requests received in the 12 month to end March 2025



2. Information Governance Performance Information April 2024 - March 2025

2.1 Data Protection Rights Requests cont'd

Fig 3: Corporate compliance with timescales for requests

Type of Request	2023/24	2024/25
Subject Access	71%	86%
Third Party	91%	95%
Other Rights Request	93%	100%

Timescales for responding

The statutory timescales for responding to data protection requests is between 30 and 90 days, depending on the complexity of the information being requested. The Council's service standards for responding to Subject Access Requests (SARs) within statutory timescales is 80% of all non complex SARs within 1 month of receipt and 70% of all complex SARs within 3 months of receipt. For other Rights Requests the service standard is 100% within 1 month of receipt. There are no statutory timescales for responding to third party requests for personal data.

Commentary

Performance in relation to handling Subject Access Requests (SARs) has improved significantly over the past 12 months due to the implementation of an improvement plan. Actions included recruitment activity and building skillsets within the existing workforce to handle complex requests. This ensures that a robust and flexible operating model is in place to meet demand. Improvement is also evident in third party access request performance (from 91% to 95%).

The majority of complex SARs continue to be care experienced related, which are challenging to fulfil within timescale due to the specialist resource required. We continue to identify complex requests as soon as possible and work with applicants to refine requests and reduce handling times.

Third party request performance has improved this year to 95% compliance despite a substantial increase in the volume of requests recorded. This is due to the implementation of revised operating model whereby some requests previously directed to council services are now managed centrally to ensure accurate reporting and compliance with legislation.

2.2 Data Protection Breaches

Fig 4: Annual number of reported data breaches

Year	Data Protection Breaches	Near Misses	Reports to the ICO
2024/25	259	33	4
2023/24	205	34	2

Data Protection Breaches

All information security incidents should be reported. The action taken will depend on the nature of the incident or breach. Incidents will either be classified as:

- A data protection breach
- Not a data protection breach
- Not a data protection breach but a near miss

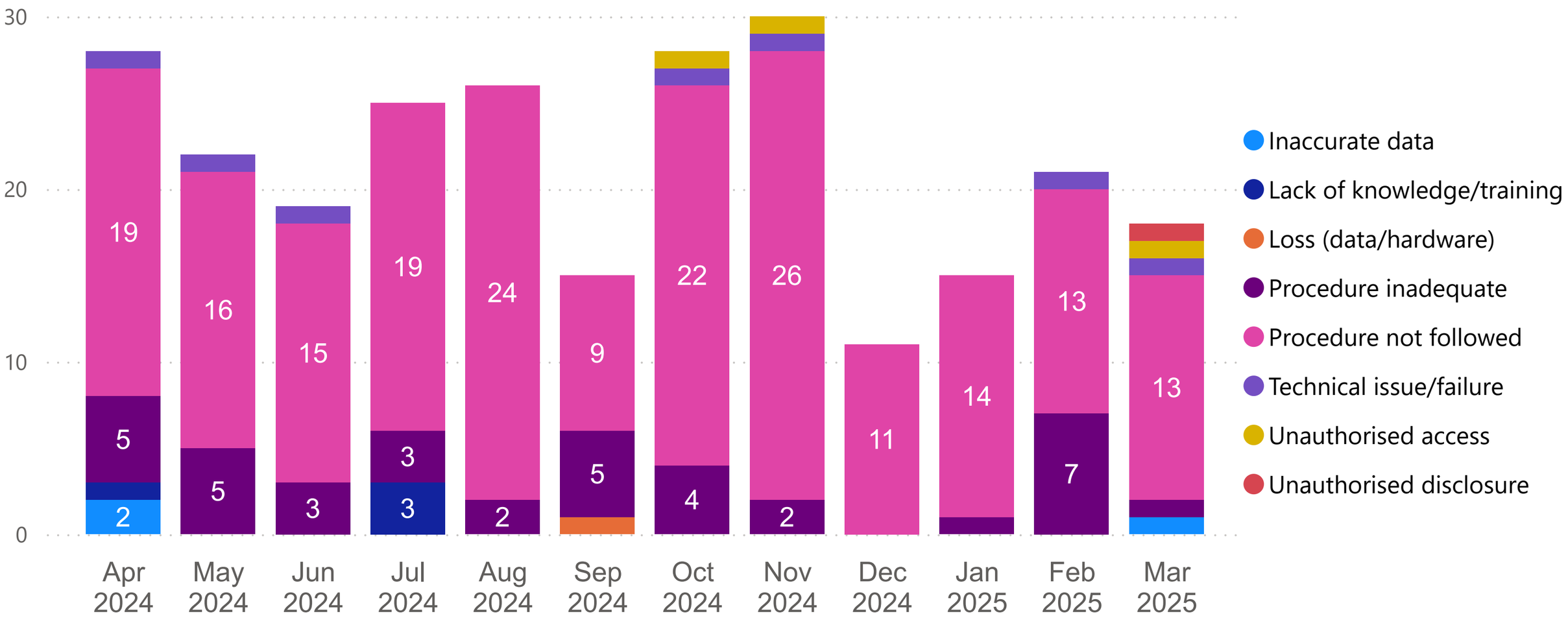
Where a breach is likely to pose a risk to the rights and freedoms of affected individuals then the Council must also notify the Information Commissioner's Office (ICO).

Commentary on number and type of breaches

This year, there has been an increase in the number of information security incidents recorded as personal data breaches. The figures indicate that there is a strong organisational awareness of what constitutes a breach and how to report one. The number of breaches remains consistent with comparable organisations based on what we know about data protection breach trends across the UK and in particular, across local government. The strong trend is that the numbers of data protection breaches has risen year on year since GDPR came into force in May 2018, and therefore the increase of recorded data protection breaches at the Council is consistent with that.

Not following existing procedures continues to be a main cause of incidents. As part of incident handling, we always look at any underlying factors which may have contributed to staff not following procedures and recommended actions to reduce the likelihood of recurrence. The Council has a baseline of controls in place which include mandatory training for all staff, regular communication in the form the Data Protection Blog and targeted support where necessary.

Figure 5: Breaches by root cause in 12 months to end of March 2025

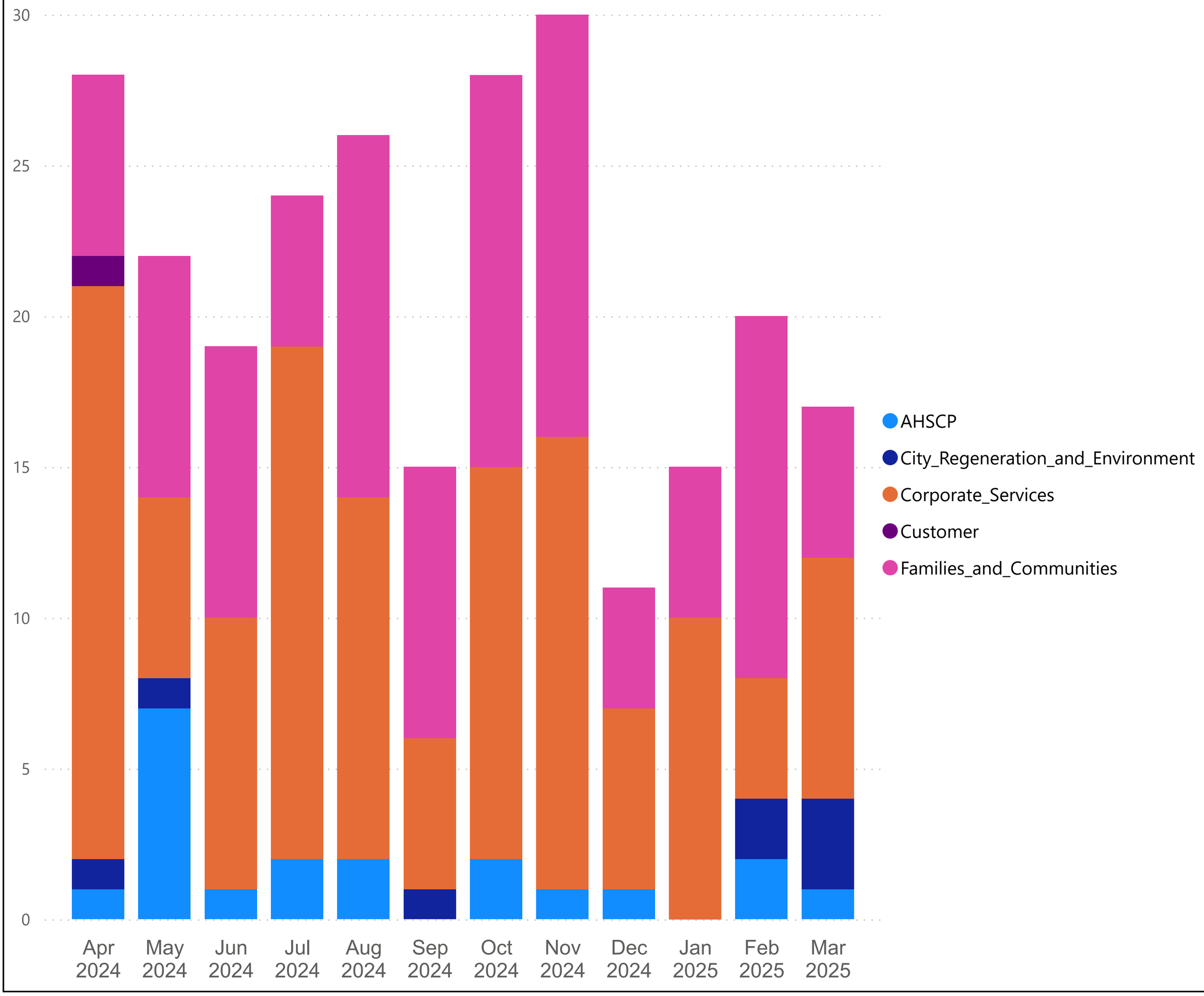


ICO Reported Breaches

The number of data breaches reported to the ICO has marginally increased in 2024/2025. When an incident has met the threshold for reporting to the ICO this is assessed and reported by the DPO. The DPO has responsibilities to monitor the compliance of the Council and has the final decision on reporting. In each case the Council has been able to evidence organisational controls sufficient to ensure that the ICO have closed with no further action being taken.

2.2 Data Protection Breaches (cont'd)

Figure 6: Breaches by Function in 12 months to end March 2025



Lessons Learned

The Council's incident handling framework means that lessons learned are identified for each incident with Service Managers, who take forward any actions identified to strengthen controls and help prevent a re-occurrence. Data protection breach data is regularly considered by Chief Officers through the Council's network of Data Forums. Lessons learned data has been made available via a real-time dashboard within the Managers Portal so it can be used across the organisation for wider learning and improvement.

Some examples of lessons learned in the past year include:

- Even when staff have appropriate training and procedures for a particular task, mistakes can still happen, particularly, when the identifying information used for the file upload is similar
- Although there are detailed procedures in place for staff around the need to double check email addresses prior to sending, mistakes are still made.

2.3 FOISA and EIR Information Requests

Fig 7: Annual number of requests received in the period

Number of requests received	2023/24	2024/25
Number of FOISA Requests	1280	1309
Number of EIR Requests	374	394

FOISA and the EIRs in brief

The Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EIR) give anyone the right to request information held by the Council, subject to certain exceptions.

Timescales for responding

The Council must respond to any request we receive within 20 working days. The Council's service standard for responding to FOISA and EIR requests within statutory timescales is 85%.

Commentary on requests received

The number of requests has increased during 2024/25. The rise may reflect an increased public awareness of their rights to access information and also be linked to public interest in some matters. Analysis has highlighted trends in requests linked to reinforced autoclaved aerated concrete (RAAC) measures and the new low emission zone (LEZ) in the city centre.

Fig 8: Request numbers in 12 months to end March 2025

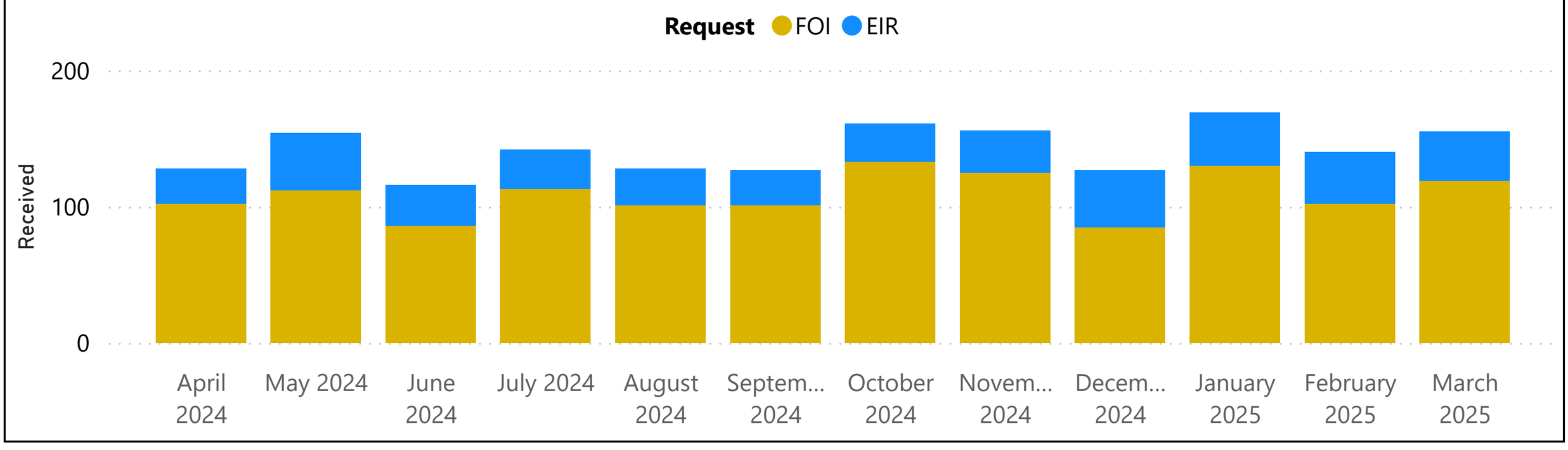


Fig 9: Compliance with timescales in the period

Report_Type	2023/24	2024/25
FOISA Requests	86%	82%
EIR Requests	89%	79%

Commentary on compliance

The volume of requests responded to within the 20-working day timescale has reduced. Performance is below target and there is a requirement to improve our compliance. An improvement plan has been developed which includes an internal campaign to raise awareness around statutory responsibility in relation to request handling.

2.4 FOISA and EIR Request Internal Reviews

Fig 10: Internal Reviews received by type in the period

Type of review received	2023/24	2024/25
No response received	19	13
Unhappy with response	22	22

Internal Reviews in Brief

If the Council does not provide a response to a FOISA or EIR request within 20 working days, or if the requester is unhappy with the response we have given, they can ask the Council to review it.

Where a requester is unhappy with our response, an internal review panel will decide whether or not to uphold the original response or overturn it.

Fig 11: Internal Review Panel outcomes in the period

Type of review outcome	2023/24	2024/25
Response overturned or amended	26	19
Response Upheld	15	13

Commentary on Internal Reviews

There has been a decrease in the number of reviews received this year which is positive.

The Access to Information Team continue to engage with applicants at the earliest opportunity to avoid escalation to review stage and services are reminded of their duty to respond to FOI/EIR requests fully and on time.

The importance of providing a clear explanation if refusing to provide information is also being highlighted with responding services.

2.5 FOISA and EIR Request Appeals

Fig 12: FOISA and EIR Appeals received and closed in the period

Type	2023/24	2024/25
Received	6	4
Closed	4	6

Right to Appeal

Where a requester remains unhappy with a response to a FOISA or EIR request after an internal review, they have the right to appeal to the Scottish Information Commissioner for a decision.

Commentary on Appeals

Of the 6 decisions made in 2024/25, 2 appeals were upheld (Aberdeen City Council decision unchanged), 2 withdrawn and 2 overturned (Aberdeen City Council decision changed).

2.6 Cyber Incidents

Fig 13: Annual number of internal cyber incidents

Incident Type	2023/24	2024/25
Internal Cyber Incident Attempts Prevented	0	0
Internal Cyber Incidents	0	0

Internal Cyber Incidents

These are risks or threats to the Council's information software, infrastructure or computer network that originate from within the premises or organisation.

Commentary on Internal Cyber Incidents

A combination of education, governance, supporting procedures and technologies have ensured the Council has not been the victim of any internal cyber incidents during this reporting period.

External Cyber Incidents

These are risks or threats to the Council's information software, infrastructure or computer network that originate from outside the premises or from the public (e.g. hackers).

Fig 14: Annual number of external cyber incidents

Incident Type	2023/24	2024/25
External Cyber Incident Attempts Prevented	7,053,507	9,586,234
External Cyber Incidents	0	0

2.7 Lost ID Badges

Fig 15: Annual number of lost ID Badges in the period

Incident Type	2023/24	2024/25
No. lost ID badges	147	153

Lost ID Badges

These are tangible and material risks or threats to the Council's information assets that originate from within the premises or organisation.

Commentary on Lost ID Badges

Facilities Management services continue to remind employees of the importance of their ID Badge, issuing 2 communications on the subject in the past financial year. The intranet post from April 2025 is the latest such post, with the link to the original post from September 2024 accessible within the April post. Despite this, the number of lost ID Badges has increased slightly in the 12 months covered in this reporting period.

Fig 16: Lost ID Badges in the period