Information Governance Management

Annual Report 2024

Senior Information Risk Owner

April 2023 - March 2024

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 2023 - March 2024

2.1 Data Protection Rights Requests

Fig 1: Annual number of requests received

Type of Request	2022/23	2023/24
Subject Access	298	316
Third Party	395	569
Other Rights Request	23	27

Data Protection Rights Requests

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

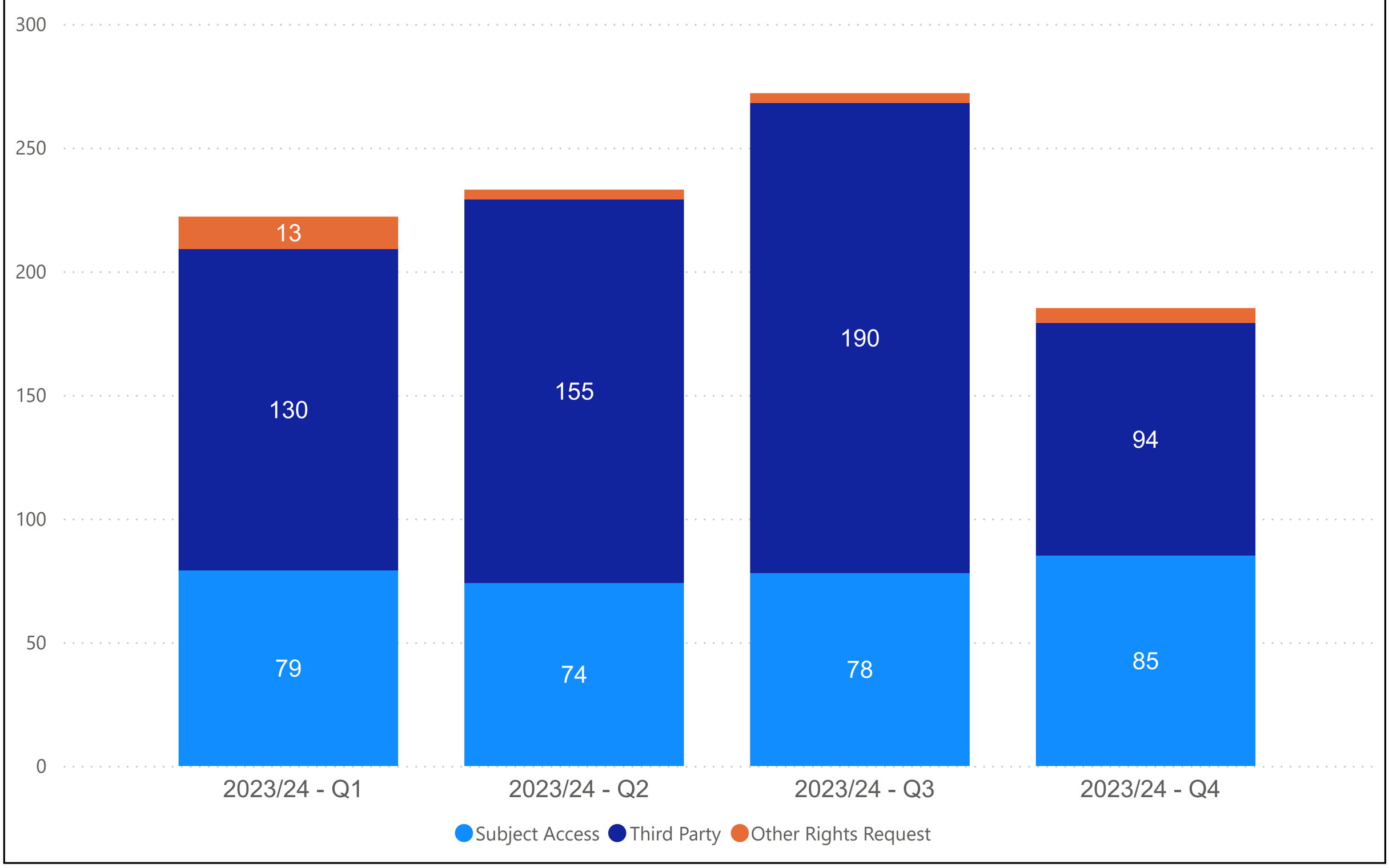
Third Party Requests

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 2024



2. Information Governance Performance Information April 2023 - March 2024

2.1 Data Protection Rights Requests cont'd

Fig 3: Corporate compliance with timescales for requests

Type of Request	2022/23	2023/24
Subject Access	68%	71%
Third Party	83%	91%
Other Rights Request	91%	93%

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

In the last year, we have made significant changes to our Subject Access process to improve our compliance. We have centralised the handling and processing of all data protection rights requests into the Access to Information team and have been liaising closely with the Information Commissioners Office to implement an improvement action plan. This includes increasing resource dedicated to handling requests from care experienced individuals and the streamlining of internal processes to maximise efficiency. We continue to work with applicants to refine requests and reduce handling time. We have seen an increase in compliance for Subject Access requests from 68% in 2022/23 to 71% in 2023/24. There was also an improvement in third party access requests from 82% in 2022/23 to 91% in 2023/24.

The majority of complex SARs continue to be care experienced which are challenging to fulfil within timescales due to the specialist resource required. The handling of these requests has been centralised under the remit of the Access to Information team and the overall management of these cases has improved. The action plan developed towards the end of 2022/23 has now been implemented to improve compliance. This included a process for identifying complex requests as soon as possible. Additional resource has been allocated to handling requests from care experienced individuals to ensure a better experience for those requesting their records. Improvement in performance is now evident and it is expected that this will continue through 2024/25.

The volume of care experience related SARs has remained high as a result of the Scottish Child Abuse Inquiry. This increased demand has been challenging to absorb, especially during periods of influxes which occur when individuals are encouraged to access their records or seek redress.

2.2 Data Protection Breaches

Fig 4: Annual number of reported data breaches

Year	Data Protection Breaches	Near Misses	Reports to the ICO
2022/23	216	33	4
2023/24	205	32	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

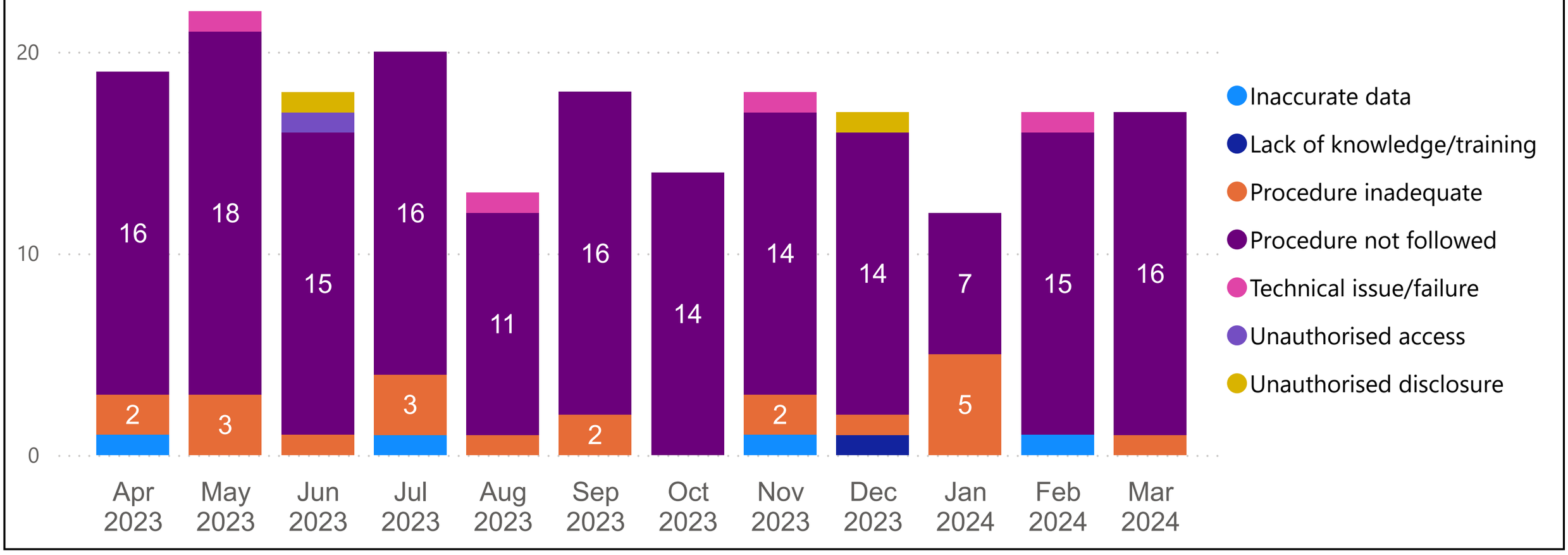
Where a breach is likely to pose a risk to the rights and freedoms of affected individuals then the Council must also notify the Information Commissioner's Office (ICO).

Commentary on number and type of breaches

There has been a decrease in the number of reported information security incidents recorded as personal data breaches at the Council this year. The figures indicate that there is a strong organisational awareness of what constitutes a breach and how to report one. The number of reported 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 reported numbers of data protection breaches has risen year on year since GDPR came into force in May 2018, and therefore the increased reported data protection breaches at the Council is consistent with that.

Not following existing procedures continues to be 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 or recurrence. The Council has a baseline of controls in place which include mandatory training for all staff, regular communication in the form of the Data Protection blog and targeted support where necessary.

Figure 5: Breaches by root cause in 12 months to end of March 2024

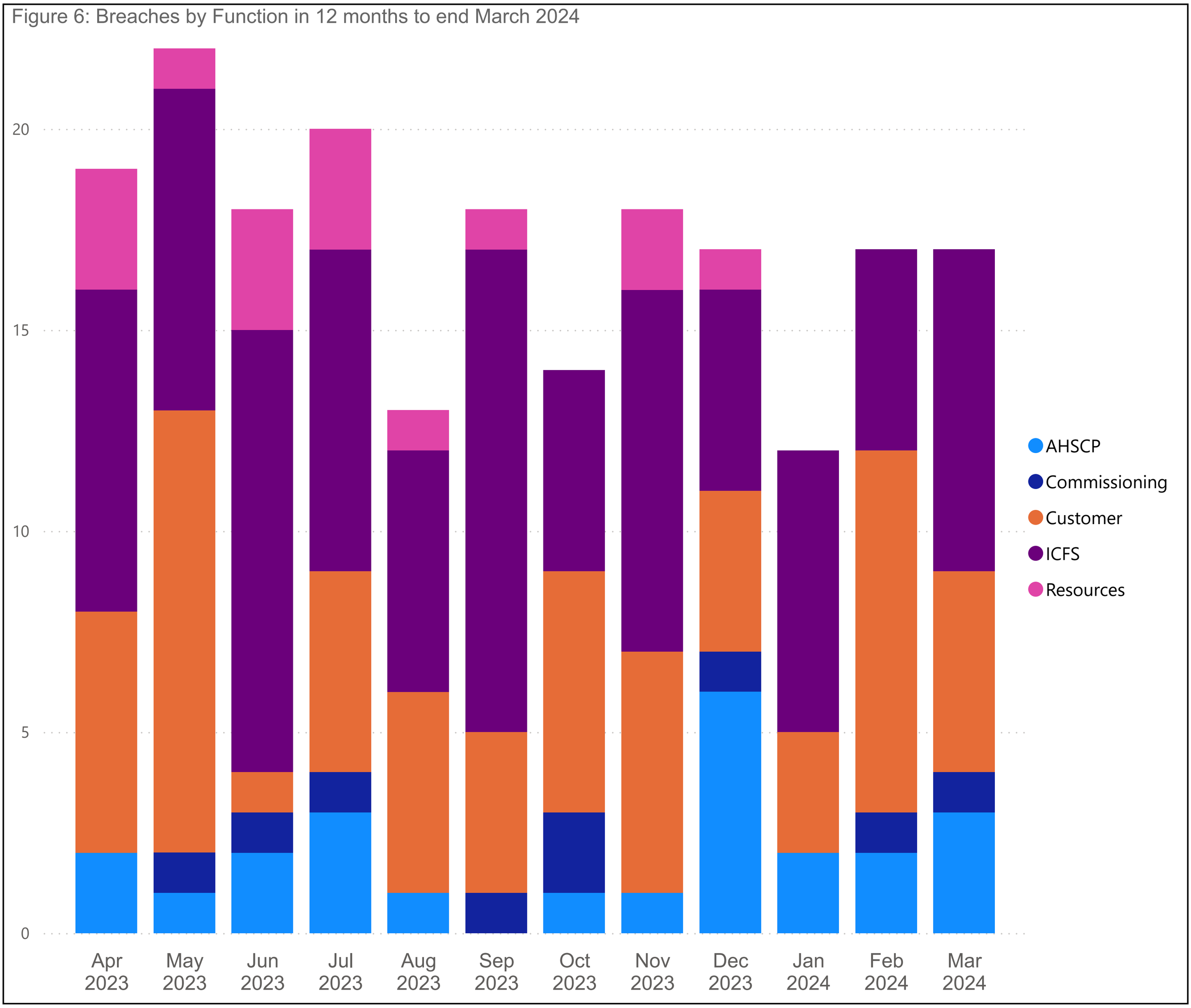


ICO Reported Breaches

The number of data breaches reported to the ICO has decreased in 2023/2024. In each case the Council has been able to evidence organisational controls sufficient to ensure that the ICO have closed all with no further action being taken.

2.2 Data Protection Breaches (cont'd)

Figure 6: Breaches by Function in 12 months to end March 2024



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.

2.3 FOISA and EIR Information Requests

Fig 7: Annual number of requests received in the period

Number of requests received	2022/23	2023/24
Number of FOISA Requests	1399	1280
Number of EIR Requests	251	374

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 2023/24. Analysis has highlighted trends in requests such as RAAC, bus gates, LEZ preparations, library and swimming closures which relate to budget decisions. An increase in media requests is also evident, for example, relating to violence in schools and other high profile areas.

Fig 8: Request numbers in 12 months to end March 2024

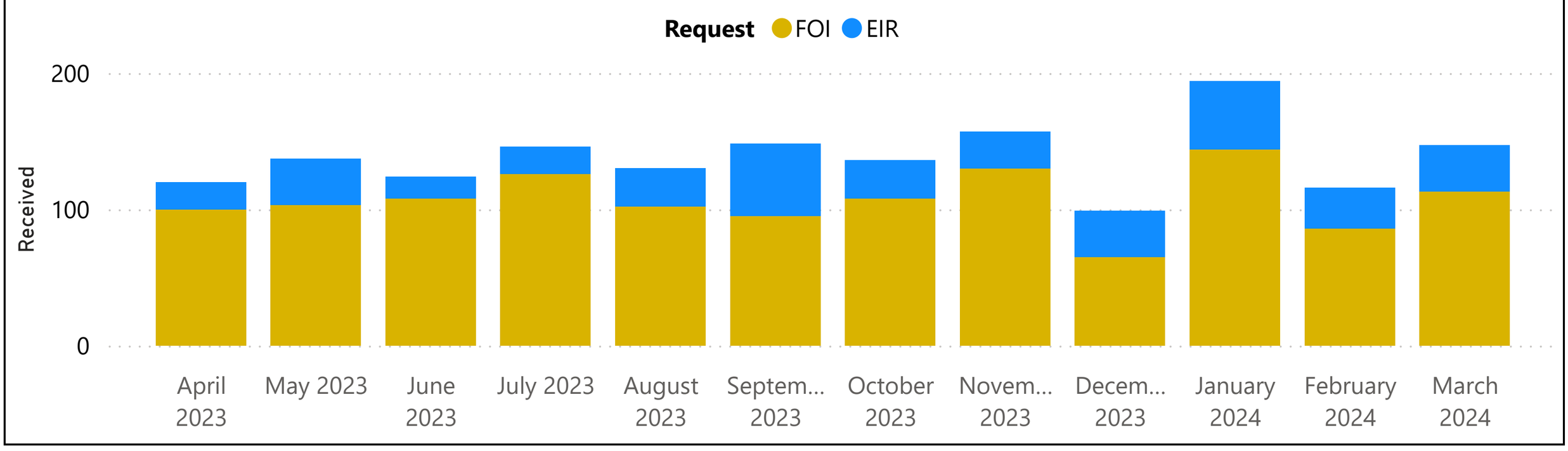


Fig 9: Compliance with timescales in the period

Report_Type	2022/23	2023/24
FOISA Requests	84%	86%
EIR Requests	83%	89%

Commentary on compliance

Compliance is slightly above target (87%). There is still scope for improvement and we are planning additional training and awareness sessions. A review of internal processes has also commenced in preparation for the implementation of a new system to manage requests.

2.4 FOISA and EIR Request Internal Reviews

Fig 10: Internal Reviews received by type in the period

Type of review received	2022/23	2023/24
No response received	18	19
Unhappy with response	31	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	2022/23	2023/24
Response overturned or amended	30	26
Response Upheld	19	15

Commentary on Internal Reviews

There has been a slight decrease in the number of reviews received this year. Half of the reviews received are due to services failing to meet response times. The Access to Information Team are continuing to focus on engaging with individuals at the earliest opportunity to avoid escalation to review stage and services are reminded of their duty to respond to FOI/EIR requests on time. It has been challenging to resource Review Panel members and activity is being undertaken to recruit additional panellists going forwards.

2.5 FOISA and EIR Request Appeals

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

Type	2022/23	2023/24
Received	2	6
Closed	3	4

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

OSIC are experiencing a large volume of appeals and this is impacting the time it takes for them to action appeals. All ongoing appeals are with OSIC for action and there is currently no action for the Council to take. It should be noted that OSIC have implemented a new approach to appeals which allows less time for ACC to respond.

2.6 Cyber Incidents

Fig 13: Annual number of internal cyber incidents

Incident Type	2022/23	2023/24
Internal Cyber Incident Attempts Prevented	0	0
Internal Cyber Incidents	3	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

Three internal cyber incidents were flagged by security defences and quickly resolved. There was no negative impact on the network.

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	2022/23	2023/24
External Cyber Incident Attempts Prevented	7,568,417	7,053,507
External Cyber Incidents	0	0

2.7 Lost ID Badges

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

Incident Type	2022/23	2023/24
No. lost ID badges	137	147

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

Steps are being taken through internal communications, to remind all employees about the importance of looking after their ID Badge, the processes they must immediately follow should they lose their ID Badge and consequences employees may face if they repeatedly lose their ID Badge. We hope that this action will see a downturn in the figures which will be reported in future cycles.

Fig 16: Lost ID Badges in the period