Information Governance Management

Annual Report 2022

Senior Information Risk Owner

April 2021 - March 2022

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 and Cyber Security risks on the Corporate Risk Register; regular updates on which are reported separately to the Council's Audit, Risk & Scrutiny Committee.

1.6   The Council's Information Governance arrangements were subject to Internal Audit, reported in February 2020. The objective of the audit was to provide assurance that the Council has adequate controls in place to mitigate the risks identified in the Corporate Risk Register and that these controls are operating as expected. The audit found that comprehensive and clear policies, procedures and mandatory training are in place and that corporate risk and related controls are being monitored by the Information Governance Group, chaired by the Council's Senior Information Risk Owner, with exception reporting to Corporate Management Team. Information Governance controls were found to be comprehensive and control assessments well-supported.

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 2021 - March 2022

2.1 Data Protection Rights Requests

Fig 1: Annual number of requests received

Type of Request	2020/21	2021/22
Subject Access	234	258
Third Party	439	327
Other Rights Request	18	17

Fig 2: Requests received in the 12 month to end March 2022

Fig 3: Corporate compliance with timescales for requests

Type of Request	2020/21	2021/22
Subject Access	76%	77%
Third Party	92%	84%
Other Rights Request	94%	88%

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.

Timescales for responding

The statutory timescale for responding to data protection requests is between 30 and 90 days, depending on the complexity of the information being requested.

There is no statutory timescale for responding to third party requests for personal data.

Commentary

In the last year, improvement has been noted in the handling of SARs within some service areas as a result of targeted training and changes to internal processes. This has resulted in an overall increase in compliance, which is positive, but performance remains below target. Requests relating to care experienced files continues to be an area where it is challenging to meet response deadlines. This is due to the specialism required to deal with such requests. A review of the associated procedures and roles/responsibilities across the teams involved is being undertaken in the coming weeks and a plan identified to seek improvement and ensure a better experience for our customers. There has been a decrease in Third Party requests and analysis into the reason for this has been undertaken but there are no evident trends.

2.2 Data Protection Breaches

Fig 4: Annual number of reported data breaches

Year	Data Protection Breaches	Near Misses	Reports to the ICO
2020/21	170	31	4
2021/22	199	20	4

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:
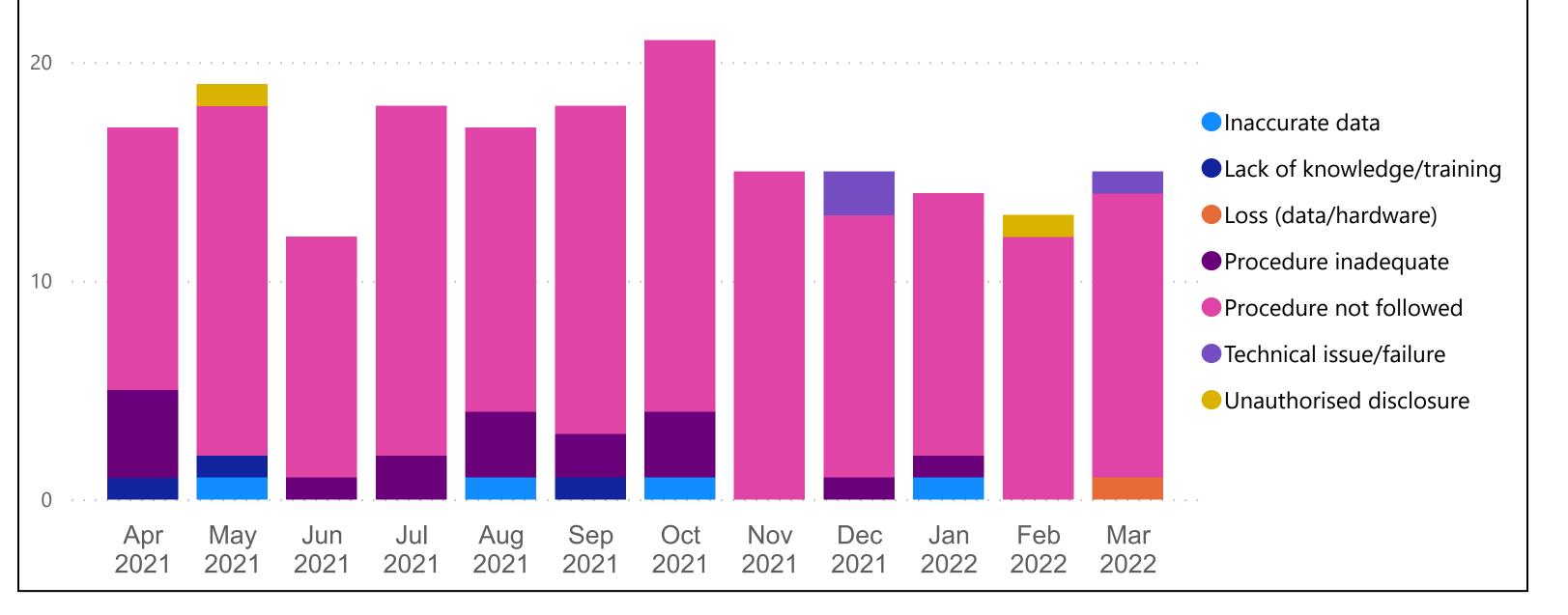
• A data protection breach
• Not a data protection breach
• Not a data protection breach but a near miss

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 an increase in reported data protection breaches 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 trend of increased reported data protection breaches at the Council is consistent with that.
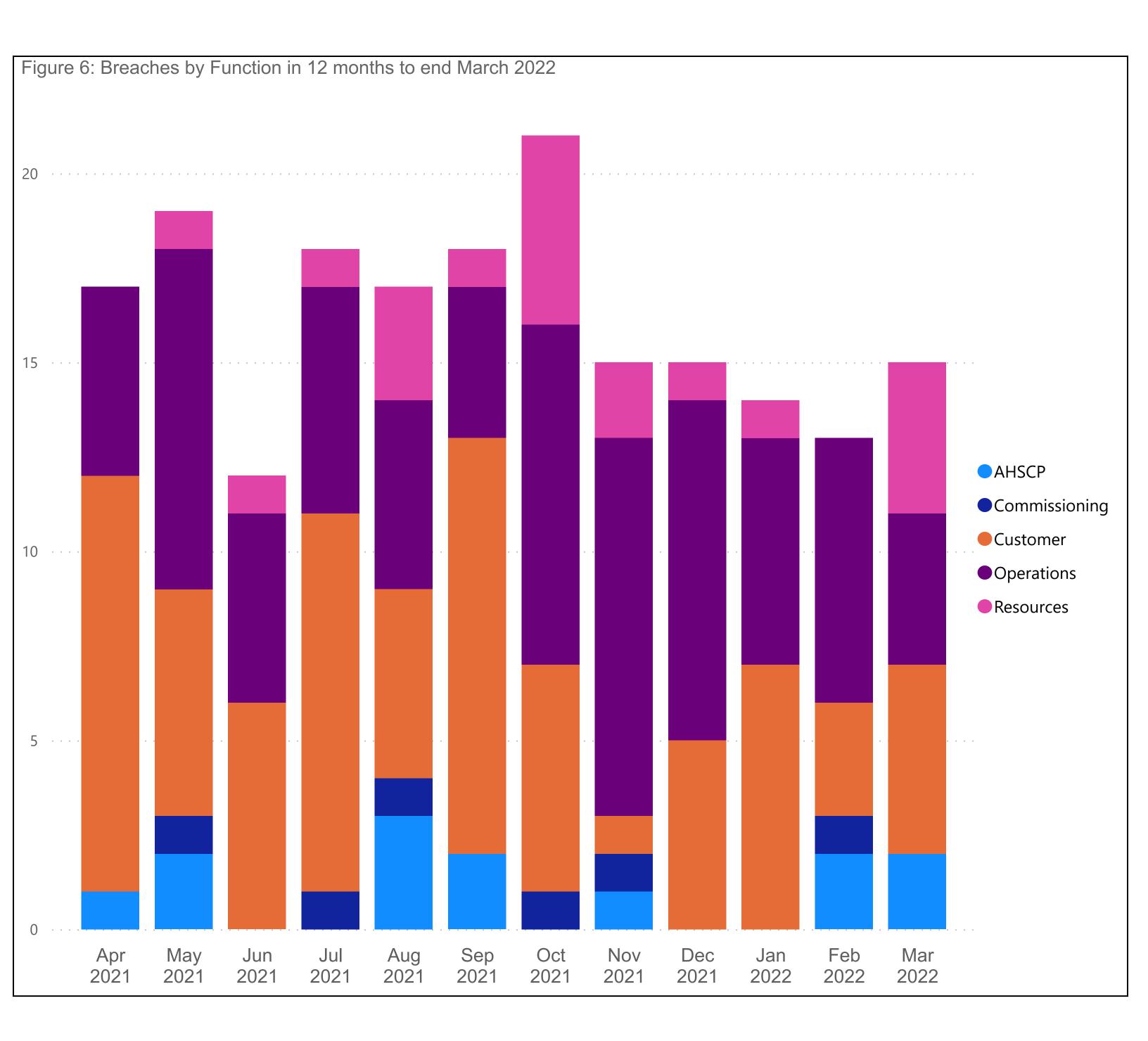
Not following existing procedures continues to be the main root cause of incidents. As part of incident handling, we always look at any underlying factors which may have contributed to staff not following procedures and recommend actions to reduce the likelihood of recurrence. The Council has a baseline of controls in place which include mandatory training for all staff, regular communications 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 2022

Legend:
● Inaccurate data
● Lack of knowledge/training
● Loss (data/hardware)
● Procedure inadequate
● Procedure not followed
● Technical issue/failure
● Unauthorised disclosure

ICO Reported Breaches

The number of data breaches reported to the ICO has remained consistent, 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 2022

Lessons Learned

The Council's 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
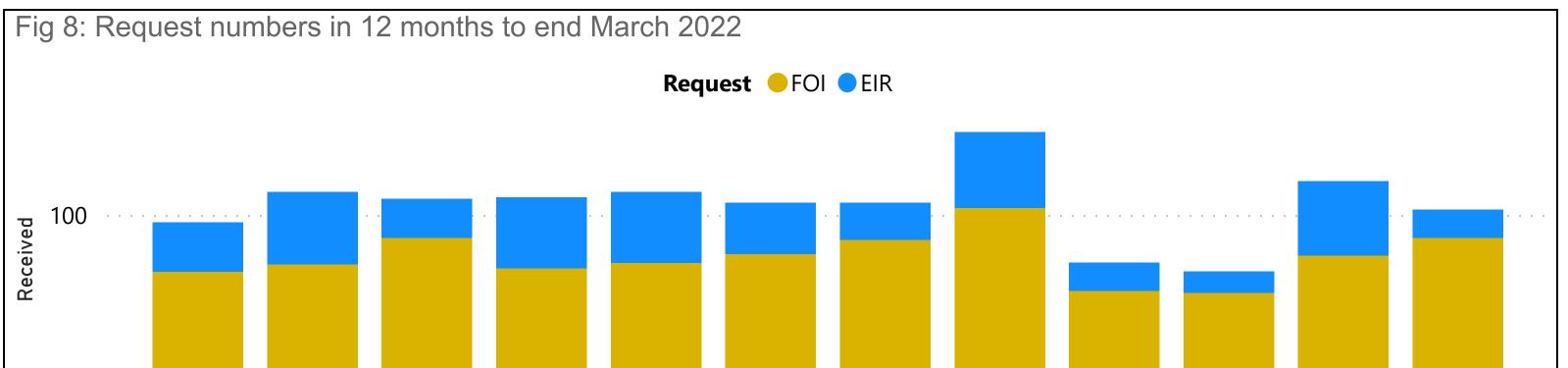
FOISA and the EIRs in brief

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.

Fig 7: Annual number of requests received in the period

Number of requests received	2020/21	2021/22
Number of FOISA Requests	903	915
Number of EIR Requests	278	350

Commentary on requests received

The number of requests has increased during 2021/22 and particularly in relation to EIRS. Analysis has highlighted trends in request such as bus gates, electric vehicles, energy transition, renewable energy and fuel usage by taxis.

Fig 8: Request numbers in 12 months to end March 2022

Fig 9: Compliance with timescales in the period

Report_Type ▼	2020/21	2021/22
FOISA	69%	89%
EIR Requests	67%	91%

Commentary on compliance

Compliance is above target and a significant improvement from the previous year due to improvements implemented, such as increased monitoring and updates to internal procedures to encourage more timely responses. There is still scope for further improvement and an action plan is in place, including targetted training, more robust management reporting and increased focus on the quality control of responses by the Access to Information Officers to ensure that responses are as helpful and clear as possible.

2.4 FOISA and EIR Request Internal Reviews

Fig 10: Internal Reviews received by type in the period

Type of review received	2020/21	2021/22
No response received	8	8
Unhappy with response	19	20

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	2020/21	2021/22
Response Upheld	15	12
Response overturned or amended	12	16

Commentary on Internal Reviews

All reviews were answered on time over the period and the number of reviews based on lateness has decreased. Where decisions were overturned due to further information being held by the Service, further guidance has been given around undertaking sufficient searches.

2.5 FOISA and EIR Request Appeals

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

Type	2020/21	2021/22
Received	2	7
Closed	1	3

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

The high level of outstanding Appeals is related to the amount of time it is taking for the Office of the Scottish Information Commissioner (OSIC) to assign Investigating Officers to cases at present. They are experiencing a large volume of appeals. In relation to the Appeal outcomes in the last 12 months, the majority have been in our favour, of the one that wasn't in our favour (Covid Business Grants), we proactively chose to release the information at appeal stage following an OSIC decision on a similar case at a different local authority.

2.6 Cyber Incidents

Fig 13: Annual number of internal cyber incidents

Incident Type	2020/21	2021/22
Internal Cyber Incident Attempts Prevented	1	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.
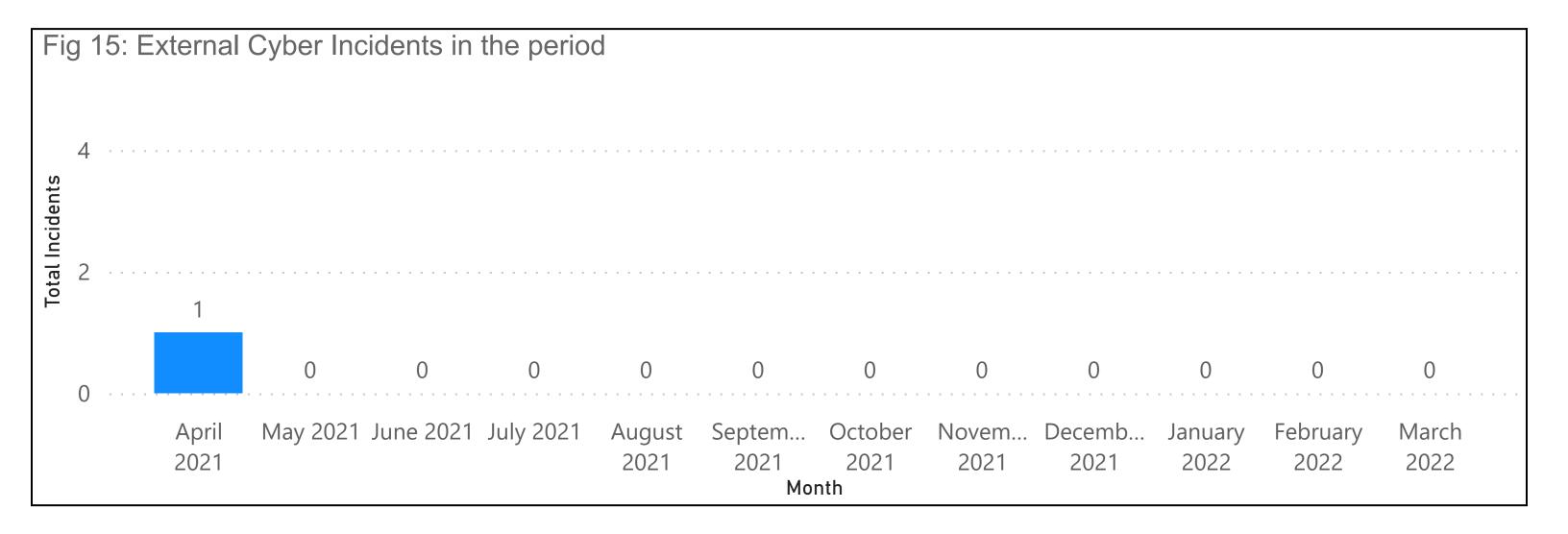
External Cyber Incidents

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).

Commentary on External Cyber Incidents

Due to failed sign in attempts from high risk countries (Russia, Korea, etc) we have developed GEO blocking. Travel to these countries will need staff to notify ICT

Fig 14: Annual number of external cyber incidents

Incident Type	2020/21	2021/22
External Cyber Incidents Prevented	15,346,510	6,306,239
External Cyber Incidents	6	1

Fig 15: External Cyber Incidents in the period

Bar chart of Total Incidents by Month: April 2021 = 1, May 2021 = 0, June 2021 = 0, July 2021 = 0, August 2021 = 0, September 2021 = 0, October 2021 = 0, November 2021 = 0, December 2021 = 0, January 2022 = 0, February 2022 = 0, March 2022 = 0

2.7 Lost ID Badges

Fig 16: Annual number of lost ID Badges in the period

Incident Type	2020/21	2021/22
No. lost ID badges	63	108

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

There has been an increase in the number of lost ID badges in the last 12 months. This increase coincides with more staff returning to office based working and figures comparable with pre COVID.

Fig 17: Lost ID Badges in the period

Incident Type ● No. lost ID badges

Month	No. lost ID badges
April 2021	15
May 2021	3
June 2021	11
July 2021	5
August 2021	10
September 2021	7
October 2021	6
November 2021	13
December 2021	6
January 2022	8
February 2022	17
March 2022	7