Information Governance Management

Annual Report 2020

Senior Information Risk Owner

July 2019 - June 2020

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. This is the fourth of these reports being presented to Committee.

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 generally 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 July 2019- June 2020

2.1 Data Protection Rights Requests

Figure 1: Annual number of requests received

Type of Request	12 months to June 2020	12 months to June 2019
Subject Access Requests	234	275
Third Party Requests	521	457
Other Rights Requests	16	15

Figure 2: Requests received in the 12 months to end of June 2020

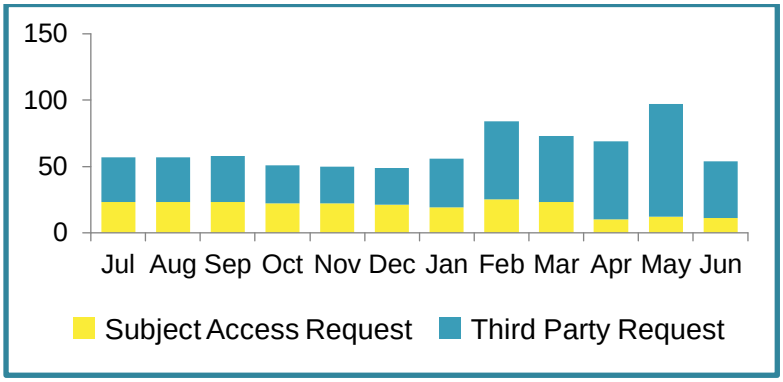


Figure 3: Corporate compliance with timescales for requests

Type of Request	12 months to June 2020	12 months to June 2019
Subject Access Requests	72%	84%
Other Data Protection Rights Requests	93%	100%

Data Protection Rights Requests

Data Protection law gives people certain rights around their data, including the right to request access to their data.

Third Party Requests

Other organisations (for example, Police Scotland or the Care Inspectorate) also make requests for 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.

Commentary on number of requests

In the last 12 months there has been a small decrease in Subject Access Requests and an increase in reported Third Party Requests. The increase in the number of third-party requests is due to a change in the reporting procedure for Council Tax requests.

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 on compliance

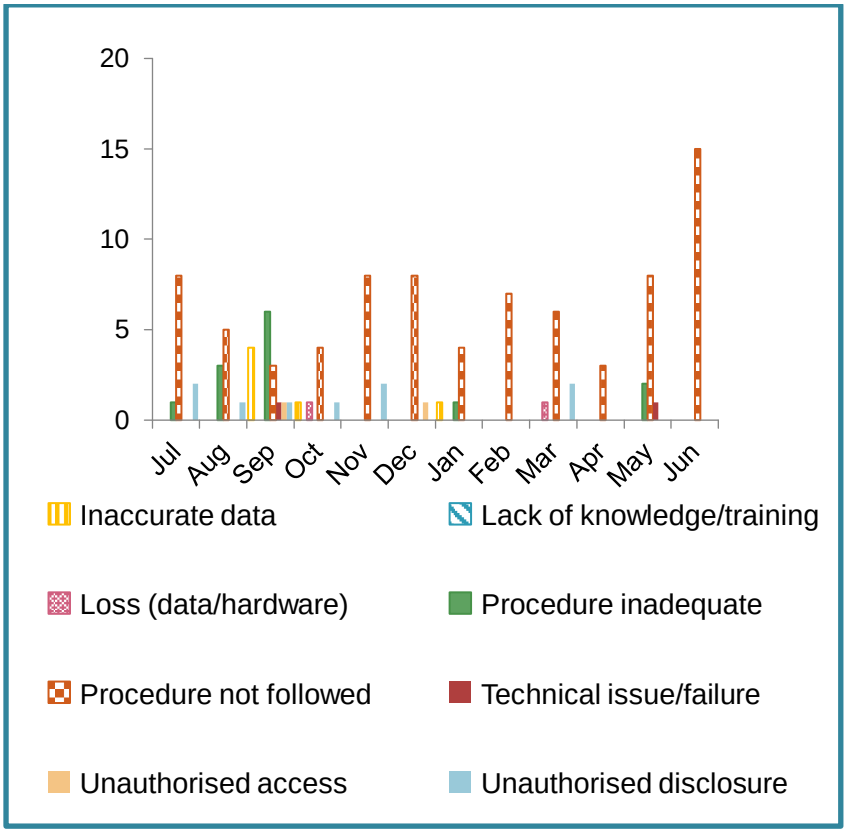
We continue to receive an increased number of requests relating to social care records which involve reviewing and redacting large, complex case files. This may may be due to a raised awareness of the Scottish Child Abuse Inquiry and access to care records. Such requests are resource intensive to complete and can exceed the statutory timescale for response.

2.2 Data Protection Breaches

Figure 4: Annual number of reported data protection breaches

Breaches	12 months to June 2020	12 months to June 2019
Data Protection Breaches	113	135
Near Misses	17	48
Reports to the ICO	2	5

Figure 5: Breaches by root cause in 12 months to end of June 2020



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 slight decrease in reported data protection breaches this year. The figures indicate that there is still a strong organisational awareness of what constitutes a breach and how to report one. The number of reported breaches remains consistent with comparable organisations.

ICO Reported breaches

There has been a decrease in the number of breaches reported to the ICO in this reporting period.

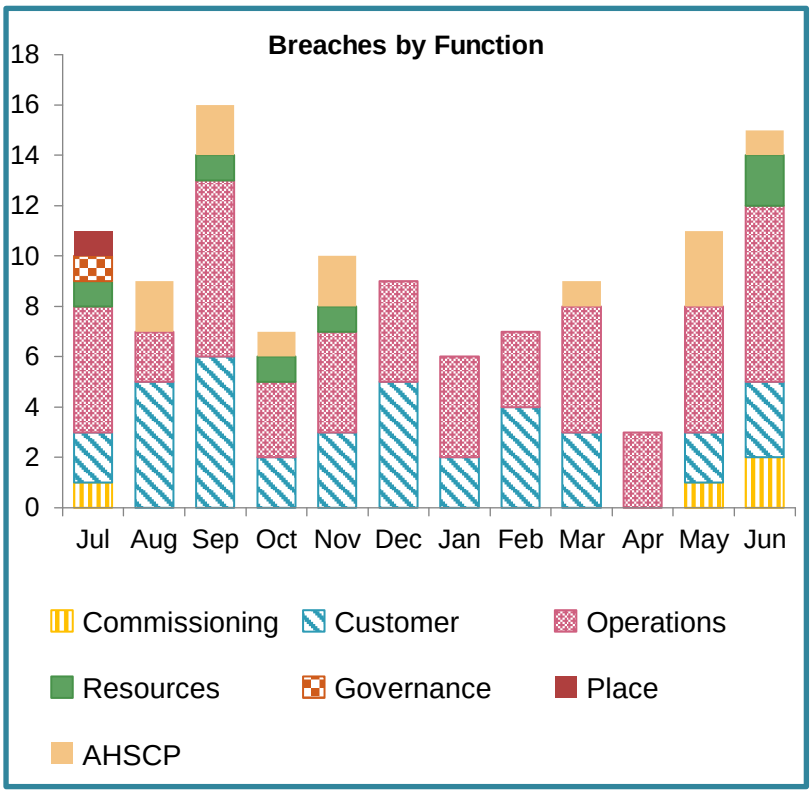
The breaches which the Council has reported to the ICO in this period have been closed with no further action being taken.

Root causes and Interventions

Compliance with Council procedures is the main root cause of incidents in this reporting period.

Appropriate action to strengthen compliance with procedures are always identified as part of the incident handling process to ensure that controls are strengthened and to reduce the likelihood of recurrence.

Figure 6: Breaches by Function in 12 months to end of June 2020



Incident and Breach Improvements

In addition to taking appropriate actions as a result of individual incidents and breaches, the Council undertakes regular monitoring of incident and breach data to identify appropriate additional actions we can take to strengthen controls. These actions are progressed through channels including the Information Governance Group, data forums led by Chief Officers, and the Council Risk Monitoring Framework.

2.3 FOISA and EIR Information Requests

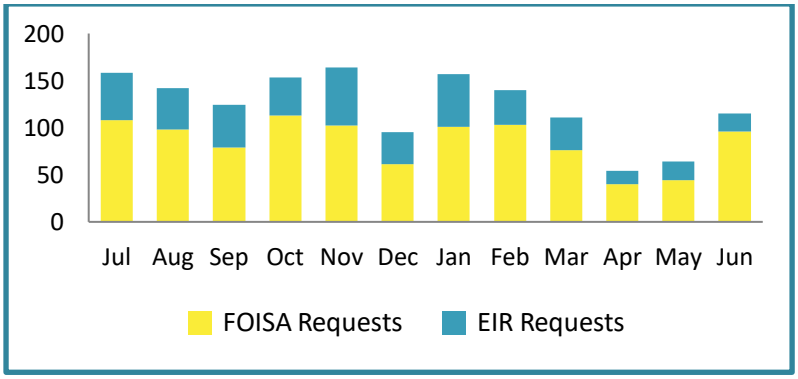
Figure 7: Annual number of requests received in the period

Number of requests received	12 months to June 2020	12 months to June 2019
Number of FOISA Requests	1021	1254
Number of EIR Requests	456	530

Figure 8: Annual Number Requester by Type received in the period

Requester by Type received	12 months to June 2020		12 months to June 2019	
Academic	30	2%	42	2%
Campaign Group	118	8%	108	6%
Commercial	259	18%	304	17%
Journalist	252	17%	353	20%
Legal	40	3%	56	3%
Politician	126	8%	160	9%
Public	641	43%	746	42%
Public Sector	11	1%	15	1%
Totals	1477	100%	1784	100%

Figure 9: Request numbers in the last 12 months



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. There was an extension to the statutory timecsales for responding to FOISA requests to 60 working days from the period of 7th April – 26th May 2020. The compliance figures in this report reflect the relevant statutory timescale.

Commentary on requests received

There was a decline in recorded requests. This was mainly due to a reduction in requests between March and May 2020, likely related to the Covid-19 pandemic.

Figure 10: Compliance with timescales in the period

Requests responded to within timescale	12 months to June 2020	12 months to June 2019
FOISA Requests	80%	88%
EIR Requests	83%	86%

Commentary on compliance

Compliance for FOI requests has fallen. This is primarily due to a dip in compliance due to a change in legislative deadlines (as described above the deadline changed from 60 to 20 days when some requests were already in progress and late as a result) and delays due to the Covid 19 pandemic which had an impact on resource allocation and also access to data.

The introduction of GovServices module on 1 September will reduce processing times which should lead to an improved compliance rate.

2.4 FOISA and EIR Request Internal Reviews

Figure 11: Internal Reviews received by type in the period

Type of review received	12 months to June 2020	12 months to June 2019
No response received	6	20
Unhappy with response	24	16

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.

Figure 12: Internal Review Panel outcomes in the period

Type of review outcome	12 months to June 2020	12 months to June 2019
Response upheld	11	13
Response overturned or amended	13	19

Commentary on Internal Reviews

The number of reviews decreased from last year.

Of the reviews, 5 were based on lateness, 1 was based on lateness and content and 23 were based on the content or use of an exemption.

Of the 24 reviews based on the use of content or exemption, 13 were overturned and an amended response was provided.

2.5 FOISA and EIR Request Appeals

Figure 13: FOISA and EIR Appeals received and closed in the period

No. of Appeals	12 months to June 2020	12 months to June 2019
Received	4	1
Closed	3	1

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

Subjects of closed appeals were e-Counting (closed in favour of the applicant); LOBO Loans (closed in favour of the applicant); and the Lord Provost's correspondence and attendance at meetings (upheld in favour of the Council).

At the end of the reporting period there was one outstanding appeal on the subject of Marischal Square, which is still to be decided by the Scottish Information Commissioner.

2.6 Cyber Incidents

Figure 14: Annual number of cyber incidents in the period

Incident Type	12 months to June 2020	12 months to June 2019
Internal Cyber Incident Attempts Prevented	0	1
Internal Cyber Incidents	1	4
External Cyber Incident Attempts Prevented	23,900,182	20,532,717
External Cyber Incidents	8	6

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

There was one incidence of password relaying recorded during the year.

Commentary External Cyber Incident Attempts

There has been a similar number of external cyber incident attempts compared with the equivalent period 12 months ago. The majority of external cyber incident attempts continue to be spam emails.

Figure 15: Internal Cyber Incidents in the period

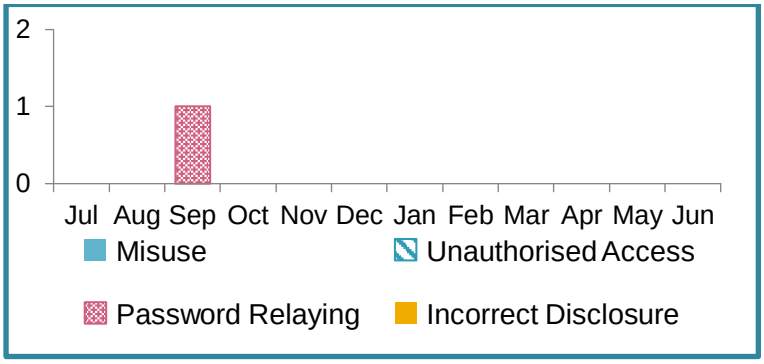
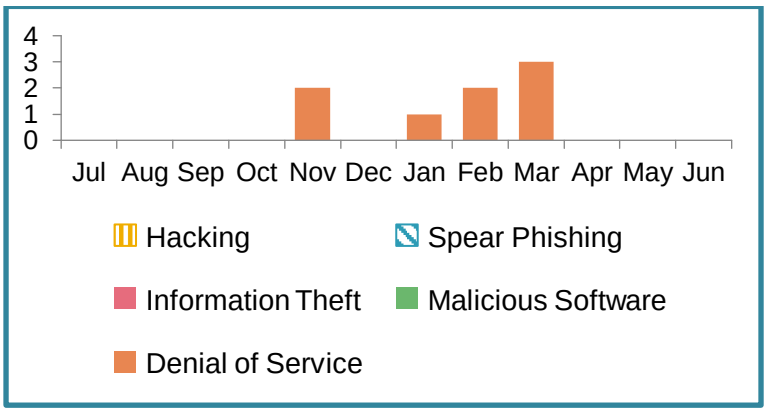


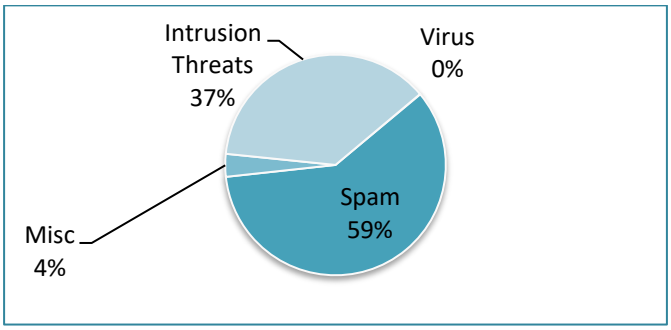
Figure 16: External Cyber Incidents in the period



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).

Figure 17: Breakdown of External Cyber Incident Attempts



2.7 Physical Incidents

Figure 18: Physical Incidents in the period

Incident Type	12 months to June 2020	12 months to June 2019
Internal Physical Incidents	128	141
External Physical Incidents	75	98

Internal Physical Incidents

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

Commentary on Internal Physical Incidents

Overall, there has been a slight reduction in the number of lost ID badges in the past 12 months. Lost badges are deactivated following notification. The decrease evident from March coincides with staff working from home where they are able to do so.

Figure 19: Internal Physical Incidents by type in the period

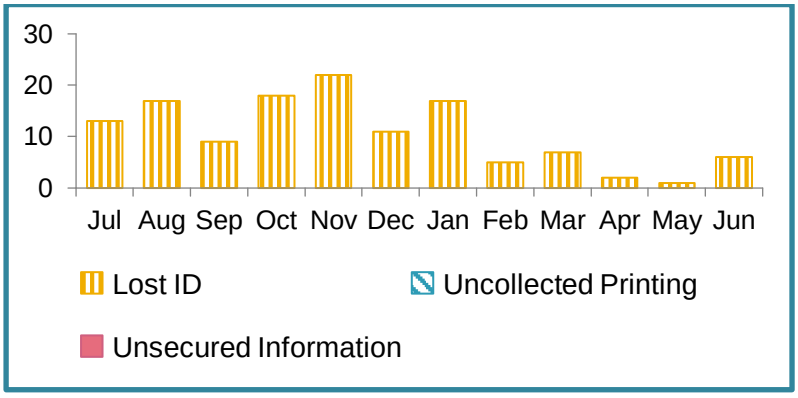
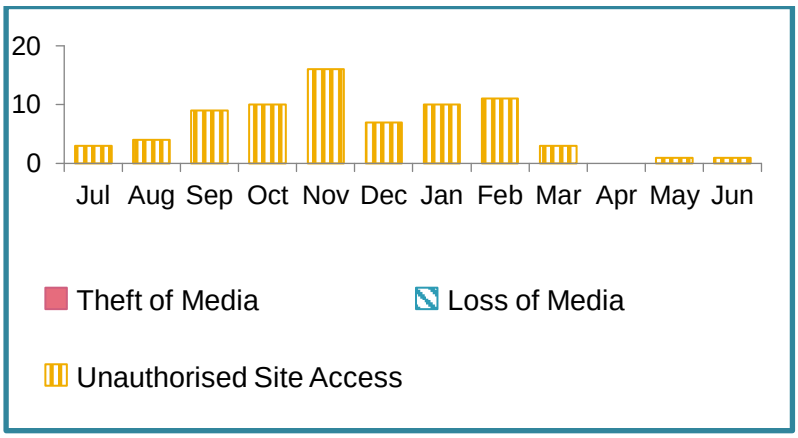


Figure 20: External Physical Incidents by type in the period



External Physical Incidents

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

Commentary on External Physical Incidents

Further information about unauthorised site access is collected via Health & Safety reporting.