# Information Governance Management

## Annual Report 2019

**Senior Information Risk Owner**

July 2018 - June 2019

# 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 third 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 ensure 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 compliance with the General Data Protection Regulation was subject to Internal Audit reported to Audit, Risk and Scrutiny Committee on 25th September 2018. The objective of the audit was to provide assurance that the Council has adequate arrangements in place, that are understood throughout the organisation, to protect the Council's information. The Council has adequate arrangements in place in terms of a Data Protection Officer; registration with the ICO; data protection impact assessments; the records of processing activities; data breach monitoring; data retention guidance; freedom of information requests; postage guidance; and confidential waste. A comprehensive range of training with appropriate exception reporting is in place. Recommendations identified to further refine privacy notices, contracts and information sharing have all been completed.

## 2. Information Governance Performance Information July 2018- June 2019

### 2.1 Data Protection Rights Requests

*Figure 1: Annual number of requests received*

| Type of Request | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| **Subject Access Requests** | 275 | 184 |
| **Third Party Requests** | 457 | 509 |
| **Other Rights Requests** | 15 | No comparable data |

*Figure 2: Requests received in the 12 months to end of June 2019*

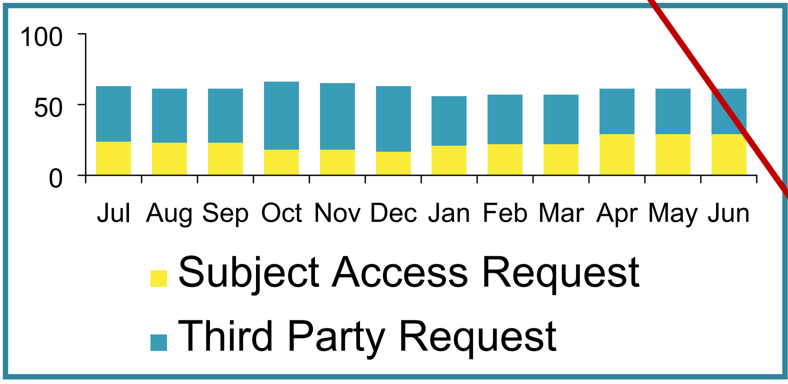


*Figure 3: Requests received by Function (July 2018-June 2019)*

| Function | Subject Access Request | Third Party Request | Other Rights Requests |
|---|---|---|---|
| **Commissioning** | 0 | 0 | 0 |
| **Customer** | 26 | 223 | 5 |
| **Operations** | 179 | 95 | 6 |
| **Resources** | 21 | 6 | 0 |
| **Governance** | 8 | 2 | 1 |
| **Place** | 7 | 70 | 0 |
| **Joint Childrens & AHSCP** | 7 | 27 | 0 |
| **AHSCP** | 17 | 27 | 3 |
| **More than one service** | 10 | 7 | 0 |

**Data Protection Rights Requests**

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

Data Rights were strengthened with GDPR becoming enforceable in May 2018.

**Third Party Requests**

Other organisations (for example, Police Scotland or the Care Inspectorate) can also make requests for customers' 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 received**

In the last 12 months there has been an increase in Subject Access Requests and a decline in Third Party Requests. This follows the same trend as last year.

*Figure 4: Breakdown of requests received by Cluster (July 2018- June 2019)*

| Cluster | Subject Access Request | Third Party Request | Other Rights Requests |
|---|---|---|---|
| **Integrated Childrens & Family Services** | 165 | 94 | 4 |
| **AHSCP** | 17 | 27 | 3 |
| **Joint Childrens & AHSCP** | 7 | 27 | 0 |
| **Operations & Protective Services** | 14 | 1 | 2 |
| **Customer Experience** | 13 | 15 | 5 |
| **Early Intervention and Community Empowerment** | 13 | 208 | 0 |
| **People & Organisation** | 21 | 6 | 0 |
| **Governance** | 8 | 2 | 1 |
| **City Growth** | 7 | 69 | 0 |
| **Strategic Place Planning** | 0 | 1 | 0 |
| **More than one Cluster/Service** | 10 | 7 | 0 |

### Timescales for responding

Subject Access and other Data Protection Rights Requests

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

Before 25 May 2018, the statutory timescale was 40 days.

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

*Figure 5: Corporate compliance with timescales for requests*

| Type of Request | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| **Subject Access Requests** | 84% | 92% |
| **Other Data Protection Rights Requests** | 100% | No comparable data |

### Commentary on compliance

Those requests which exceed the statutory timescale for responding are requests relating to social care records which can involve reviewing and redacting large and complex case files.

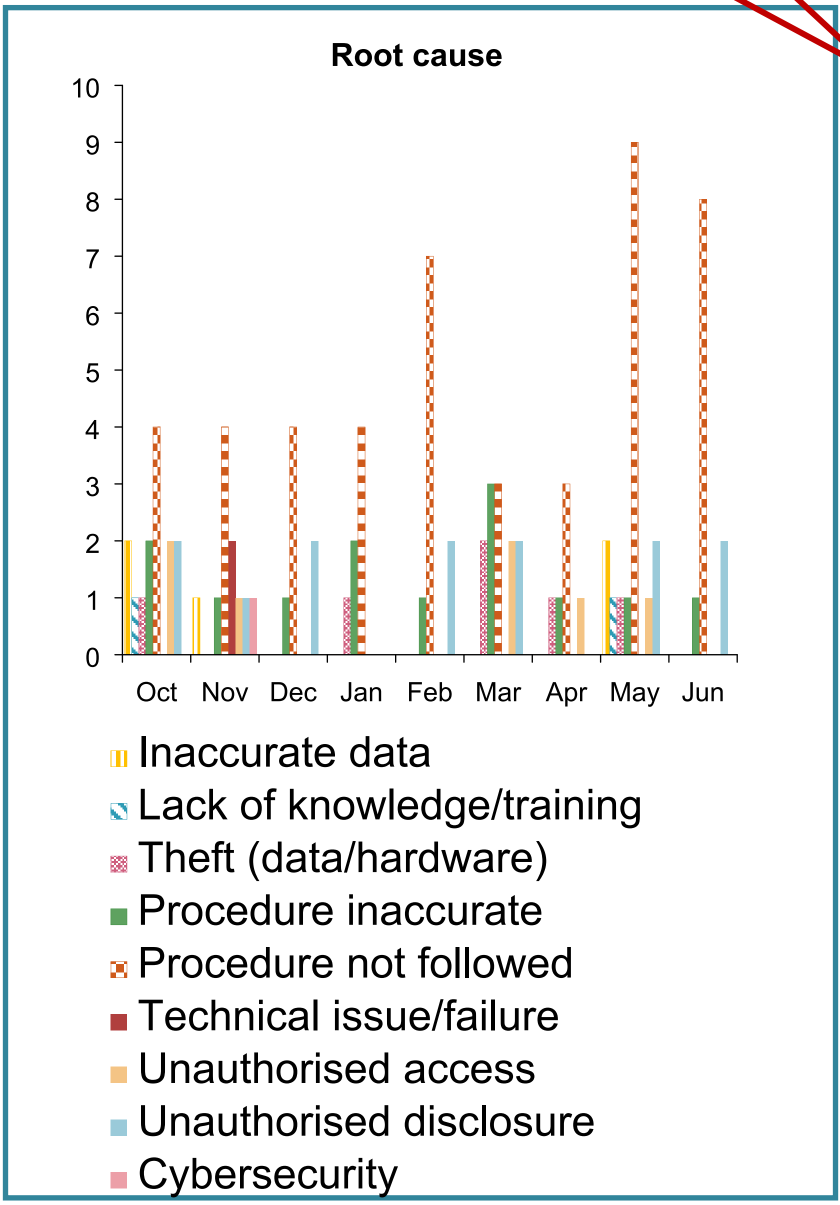
Data Protection Rights Requests are now carried out as a centralised function by the Access to Information Team.

## 2.2 Data Protection Breaches

*Figure 6: Annual number of reported data protection breaches*

| Breaches | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| **Data Protection Breaches** | 135 | 61 |
| **Near Misses** | 48 | No comparable data |
| **Reports to the ICO** | 5 | 1 |

*Figure 7: Breaches by root cause over the last 9 months*



**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 which is likely to be attributable to increased organisational awareness of what constitutes a breach and how to report one. This increase is consistent with comparable organisations.

**ICO Reported breaches**

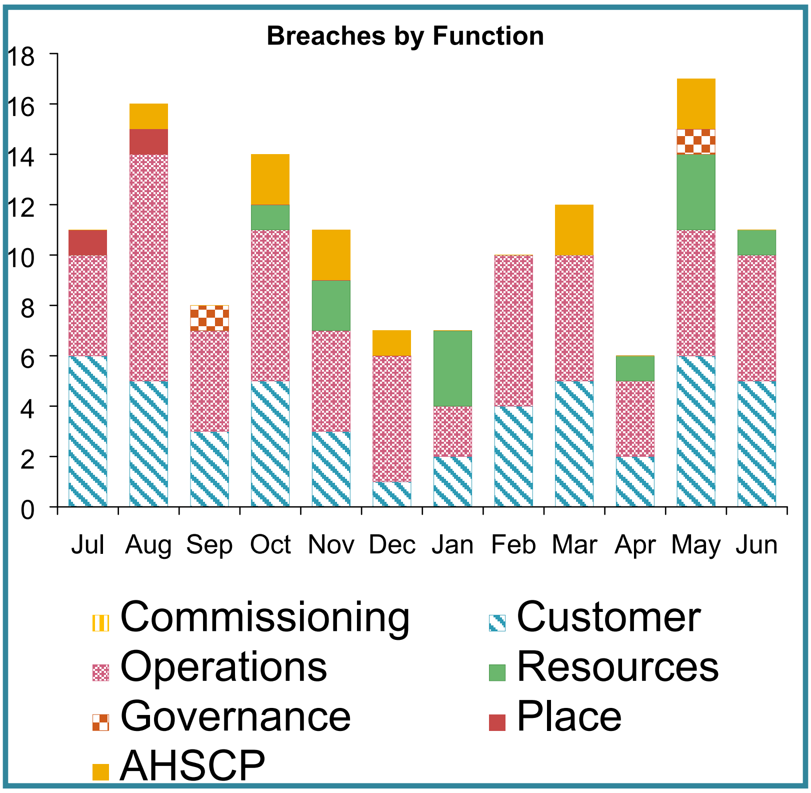
ICO notification requirements changed when GDPR became enforceable in May 2018 which provides context for the increase in ICO notified breaches from 2018. All breaches which the Council has reported to the ICO within this reporting period have been closed with no further action being taken.

**Root causes and Interventions**

In October 2018 a revision of breach root cause classifications was implemented to ensure that in every case following an incident or breach the right actions are being taken to strengthen the Council's controls and to help prevent a recurrence.

Council procedures are a root cause area that continue to be targeted to ensure they align to professional practice.

*Figure 8: Breaches by Function in 12 months to end of June 2019*



**Incident and Breach Improvements**

As part of the monitoring and interventions required to strengthen the Council's controls and prevent a recurrence, targeted action plans are now being implemented within Clusters directly affected

## 2.3 FOISA and EIR Information Requests

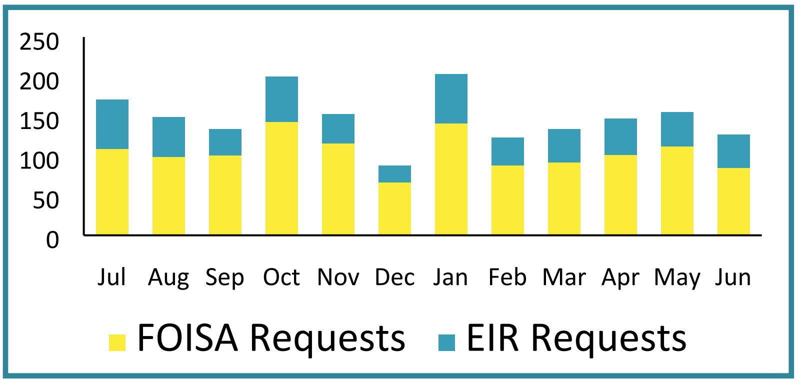
*Figure 9: Annual number of requests received in the period*

| Number of requests received | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| Number of FOISA Requests | 1254 | 1348 |
| Number of EIR Requests | 530 | 636 |

*Figure 10: Annual Number Requester by Type received in the period*

| Requester by Type received | 12 months to June 2019 | | 12 months to June 2018 | |
|---|---|---|---|---|
| Academic | 42 | 2% | 48 | 2% |
| Campaign Group | 108 | 6% | 130 | 7% |
| Commercial | 304 | 17% | 282 | 14% |
| Journalist | 353 | 20% | 377 | 19% |
| Legal | 56 | 3% | 96 | 5% |
| Politician | 160 | 9% | 187 | 9% |
| Public | 746 | 42% | 844 | 43% |
| Public Sector | 15 | 1% | 18 | 1% |
| Totals | 1784 | 100% | 1984 | 100% |

*Figure 11: 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.

**Commentary on requests received**

The decrease in recorded requests is largely due to changes in how requests are logged and the categorisation of requests, for example the handling of a request using an alternative information rights process such as a data protection rights request.

*Figure 12: Compliance with timescales in the period*

| Requests responded to within timescale | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| FOISA Requests | 88% | 94% |
| EIR Requests | 86% | 98% |

**Commentary on compliance**

The compliance rate for April and May in 2019 fell for the following reasons:

Focus has shifted to statutory compliance on SARS, whilst ensuring FOI remains a high performing area.

Some delays are caused where multiple services are involved – solutions are being addressed.

## 2.4 FOISA and EIR Request Internal Reviews

*Figure 13: Internal Reviews received by type in the period*

| Type of review received | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| No response received | 20 | 10 |
| Unhappy with response | 16 | 39 |

*Figure 14: Internal Review Panel outcomes in the period*

| Type of review outcome | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| Response upheld | 13 | 32 |
| Response overturned or amended | 19 | 17 |

**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.

## 2.5 FOISA and EIR Request Appeals

*Figure 15: FOISA and EIR Appeals received and closed in the period*

| No. of Appeals | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| **Received** | 1 | 3 |
| **Closed** | 1 | 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**

One appeal was received in relation to the Kingsford Stadium. ACC's response was upheld by the Scottish Information Commissioner.

## 2.6 Cyber Incidents

*Figure 16: Annual number of cyber incidents in the period*

| Incident Type | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| **Internal Cyber Incident Attempts Prevented** | 1 | 2 |
| **Internal Cyber Incidents** | 4 | 3 |
| **External Cyber Incident Attempts Prevented** | 20532717 | 40790746 |
| **External Cyber Incidents** | 6 | 12 |

**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 were 3 incidences of password relaying recorded during the year. There has been one instance of misuse.

**Commentary External Cyber Incident Attempts**

There has been a significant reduction in the 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 17: Internal Cyber Incidents in the period*

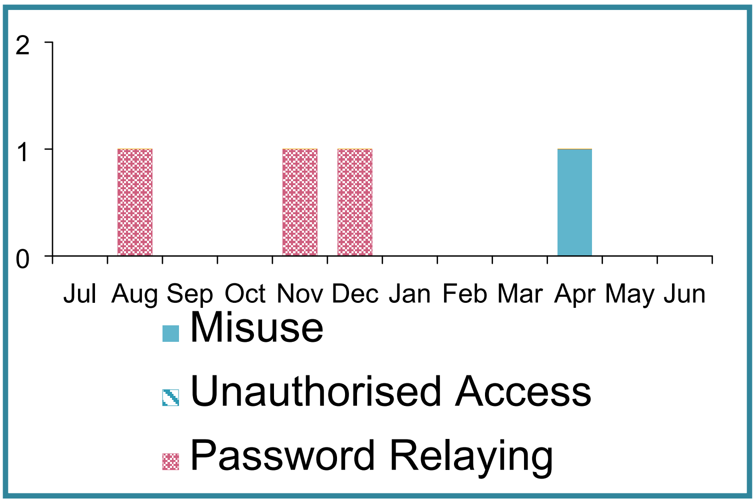
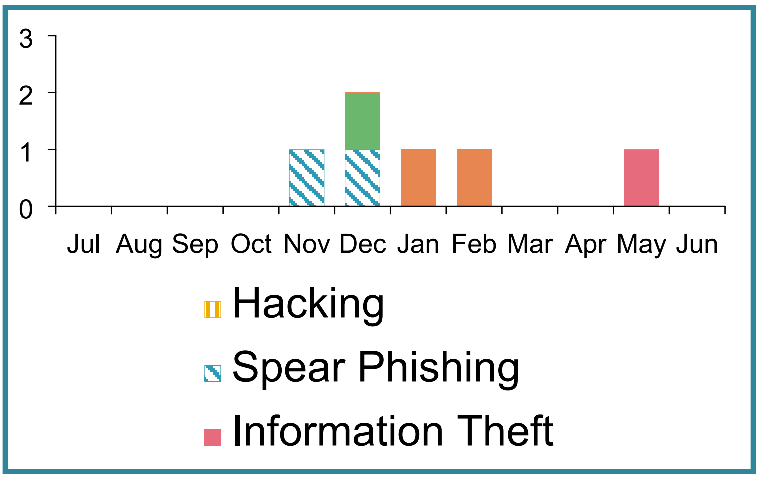


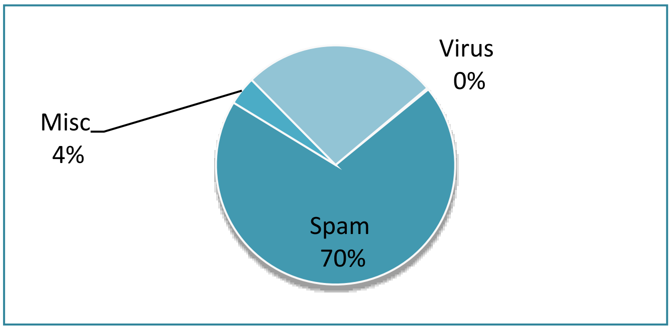
*Figure 18: External Cyber Incidents in the period*



**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 19: Breakdown of External Cyber Incident Attempts*



## 2.7 Physical Incidents

*Figure 20: Physical Incidents in the period*

| Incident Type | 12 months to June 2019 | 12 months to June 2018 |
|---|---|---|
| Internal Physical Incidents | 141 | 153 |
| External Physical Incidents | 98 | 72 |

*Figure 21: Internal Physical Incidents by type in the period*

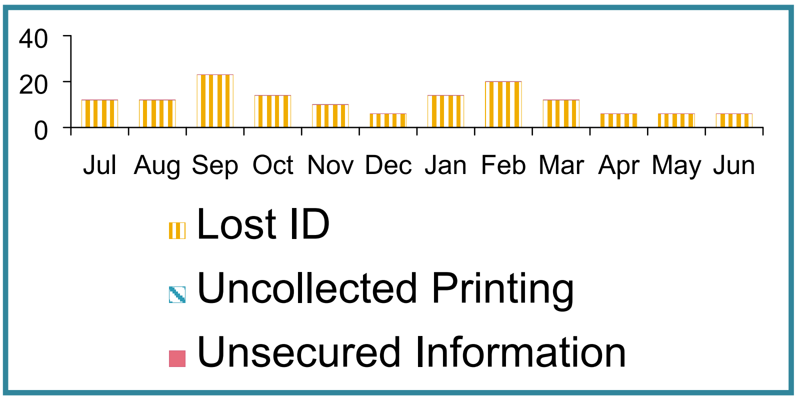
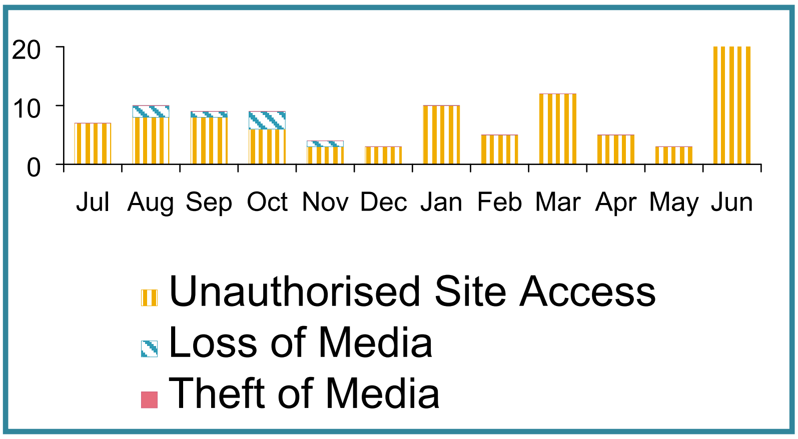


*Figure 22: External Physical Incidents by type in the period*



**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.

**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.