NOT FOR PUBLICATION

This report is circulated for consultation purposes only and must not be discussed or the contents released to anyone or any organisation outwith the Council. You should only discuss this with authorised Council employees. If you are in any doubt about who you are able to disclose this information to please contact the report author or your Director or Head of Service. If you are a member of a trade union and you are being consulted on this report as part of the Council's formal consultation procedures please adhere to these arrangements and contact the Head of Human Resources if you require any further advice.

ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk & Scrutiny
DATE	27 September 2016
DIRECTOR	Richard Ellis
TITLE OF REPORT	Information Governance Management and Reporting Arrangements
REPORT NUMBER	CG/16/109
CHECKLIST COMPLETED	Yes

1. PURPOSE OF REPORT

To seek Committee approval of the proposed Council's information governance management and reporting arrangements.

2. RECOMMENDATION(S)

It is recommended that the Committee:

i) Note the information contained in this report, and;

ii) Approve the proposed changes for oversight and reporting of information governance.

3. FINANCIAL IMPLICATIONS

There are no financial implications arising directly from this report.

4. OTHER IMPLICATIONS

None.

5. BACKGROUND/MAIN ISSUES

The Council is reviewing and redefining its arrangements for Information Governance Management and Reporting as part of its wider Governance Review.

The Council's information is a critical asset, underpinning service delivery, used by all staff, and affecting all customers and their experience of the Council. This means that getting our information governance arrangements right is fundamental to the Council's ability to effectively use information to transform and modernise the way we do business.

Understanding the nature of the risks to the Council from failure to govern our information properly is critical. The impact can be very serious, and in some cases may place the individuals we serve at risk of harm. Protecting our information appropriately is crucial (the Council block over 300,000 cyber threats every month) but this is only one aspect of governing our information properly: making sure that our information is joined up and integrated where it needs to be, shared when it should be, kept for the right amount of time, and is open and transparent whenever it can be, are all essential components of good information governance practice.

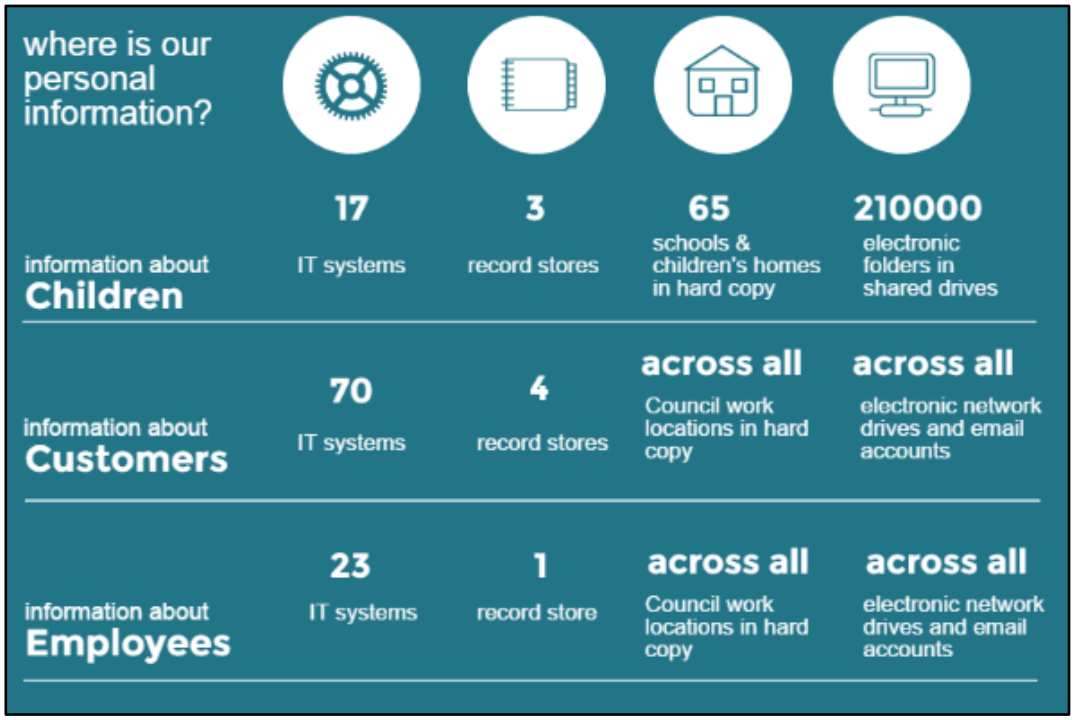
Failure to govern our information properly may also result in reputational damage and in financial penalties: the maximum fine for breaches of Data Protection is currently £500,000, but this is set to rise when the new General Data Protection Regulation comes into force in 2018.

The Council needs to be able to evidence robust information governance arrangements to comply with our statutory and legislative responsibilities, which include: in the Data Protection Act 1998, Freedom of Information (Scotland) Act 2002, Environmental Information (Scotland) Regulations 2004, Re-use of Public Sector Information Regulations 2015, Public Records (Scotland) Act 2011, the Computer Misuse Act (1990), the Copyright, Designs and Patents Act (1988), the Human Rights Act (1998), the Regulation of Investigatory Powers (Scotland) Act 2000; Public Sector Network (PSN) Compliance, PCI (Payment Card Industry) Compliance.

These compliance areas are interdependent rather than standalone, because the Council's ability to comply with one set of legislative requirements is dependent on being able to evidence good practice across a range of information governance areas. This is in the context of the Council's large and complex information landscape, which consists of:

- 400 applications
- 11 million electronic files
- 9km of hardcopy files
- 19,000 Access databases
- 500 servers
- 3,000 laptops

Within this context, the council holds its most high value and high risk personal information about our children, customers and employees across a wide range of systems and locations:



To meet our statutory obligations within this context, and to make the best use of our resources, we need a Council-wide, joined-up approach to information governance.

The following details a proposal that will deliver a single point of oversight which will provide strategy and leadership, and allow for joined-up, targeted initiatives to improve performance. With an overview of performance across the information governance landscape, meaningful reporting can be delivered to the correct audience among senior management, who can in turn support the teams responsible for compliance.

Information Governance Arrangements

Scope

These arrangements bring together the following assurance areas:

- Data Protection
- Freedom of Information & Environmental Information
- Information Security
- Information and Data Management
- Open Data and Information Re-use

Approach

The Council's Information Governance approach (**Appendix 2**) is focussed on three key areas:

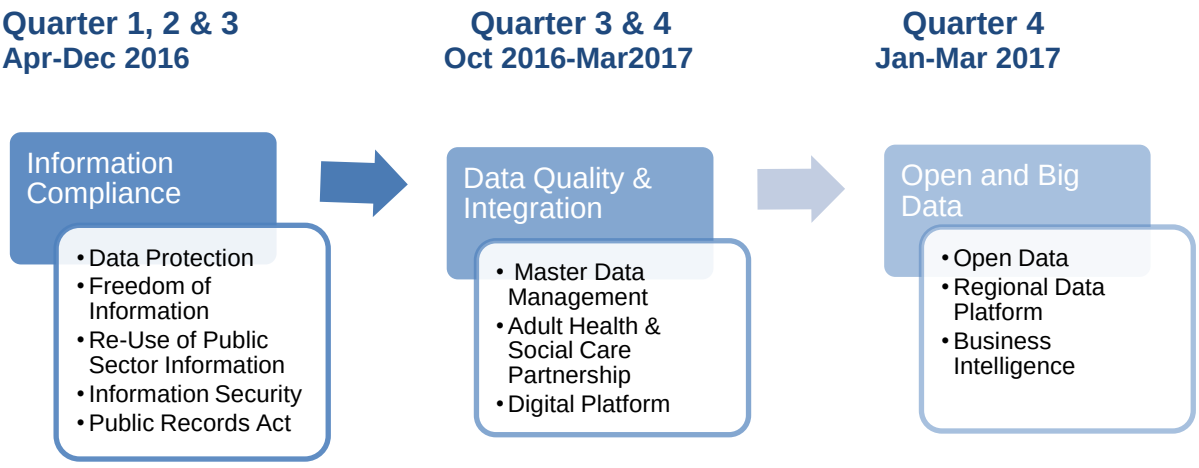
- Systems and Processes
- People and Behaviour
- Adapting and Learning

For each of these areas, the Information Governance Group will monitor the effectiveness of the controls, measures and activities in place, so the Council is able to:

- evidence policy, procedure and system effectiveness
- identify policy, procedure, system and capability gaps and address them
- chart progress on information governance improvement programme
- monitor and manage training effectiveness and completion
- act quickly and appropriately to breaches, incidents, issues or complaints and to make any required remedial change
- respond appropriately to relevant legislative or business change

The Group's focus will be:

1. Ensuring compliance with information legislation
2. Improving data quality and integration through master data management
3. Transformation through open and big data



For each of the priority areas, and in line with its defined approach, the Information Governance Group will:

- Conduct a review of the systems and processes in place to make sure that they are up to date and fit for purpose, and that the right measures are in place to evidence their effectiveness.
- Conduct a review of the training, awareness and engagement activities in place to make sure that they are up to date and fit for purpose, and

that the right measures are in place to monitor their uptake and effectiveness.
- Conduct a of review the way we respond to incidents, breaches, issues, complaints and changes in legislation to make sure that we are taking the right action and can evidence that we are learning and adapting where we need to.

Where issues and gaps are identified the Information Governance Group will agree an information governance improvement programme outlining:

- What action needs to be taken
- Who will be responsible for completing the action
- What other stakeholders will be involved in completing the action
- When it will be completed

After each priority area has been subject to review by the Information Governance Group, it will be subject to monitoring on an ongoing basis, to ensure that the measures we have in place continue to be up to date, appropriate and effective.

The information governance improvement programme will be monitored against the Council's Information Risk Register, to measure and manage the impact of the programme in control and mitigation of the Council's information risks.

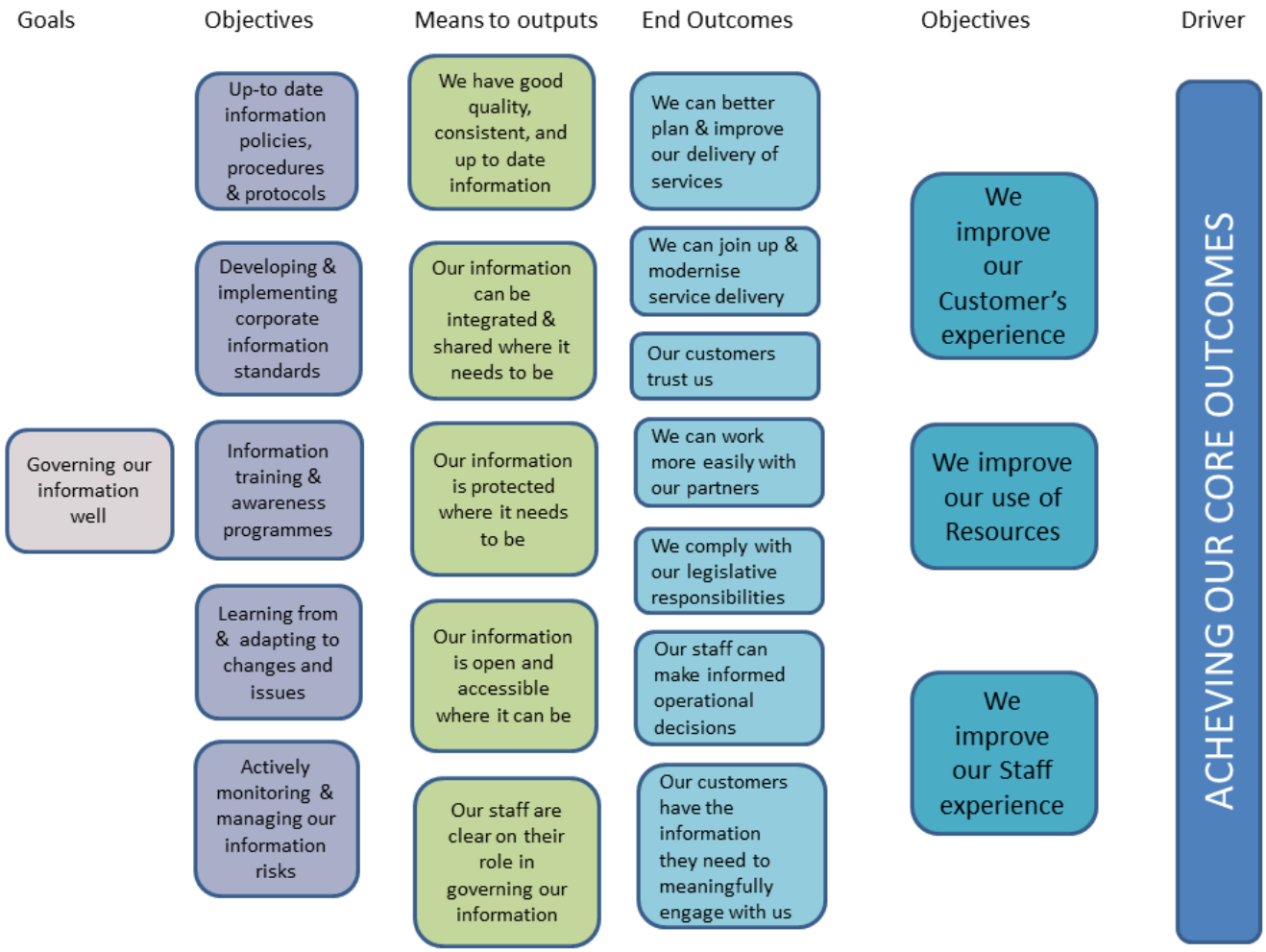
Governance

The Information Governance Group will drive the Council's information governance agenda. The Group is chaired by the Council's Senior Information Risk Owner (SIRO), a role undertaken by the Head of IT & Transformation. The Group includes representatives from across the Council, as well as from each assurance area within scope (see **Appendix 3:** Terms of Reference for the Information Governance Group).

Reporting

Each assurance area will report through the Corporate Performance Dashboard. The Information Governance Group will manage and monitor the effectiveness of the Council's Information Governance Framework, and will report quarterly to the CMT (beginning Sept. 2016, see **Appendix 1**). The SIRO will also report annually to the Council's Audit, Risk & Scrutiny Committee. It is proposed that these reporting arrangements will replace the current quarterly Data Protection reporting to Committee.

6. IMPACT



An Equality and Human Rights Impact Assessment and Privacy Impact Assessment has been undertaken.

7. MANAGEMENT OF RISK

The Information Governance Group and Framework exist to manage and mitigate the Council's information risks. Compliance will be reported to CMT quarterly and Audit, Risk and Scrutiny Committee on an annual basis.

8. BACKGROUND PAPERS

Information Management Strategy
Information Security Policy
ICT Acceptable Use Policy
Freedom of Information Policy
Data Protection Policy
Information Lifecycle Management Policy & related policy suite
Records Management Plan

9. REPORT AUTHOR DETAILS

Caroline Anderson
IT & Transformation
canderson@aberdeencity.gov.uk
01224 522521

Appendix 1: Information Governance Report Template

See Overleaf

ABERDEEN
CITY COUNCIL

Information Governance Management

Quarterly Performance Report

Information Governance Group

Q1 2016/7

Executive Summary: Information Governance Improvement Programme

Improvement		Action	Date	Owner	R/A/G status	Commentary
Systems & Processes	Review systems and processes					
People & Behaviour	Review training, awareness and engagement activities					
Adapting & Learning	Review response to incidents, breaches, issues, complaints and changes in legislation					

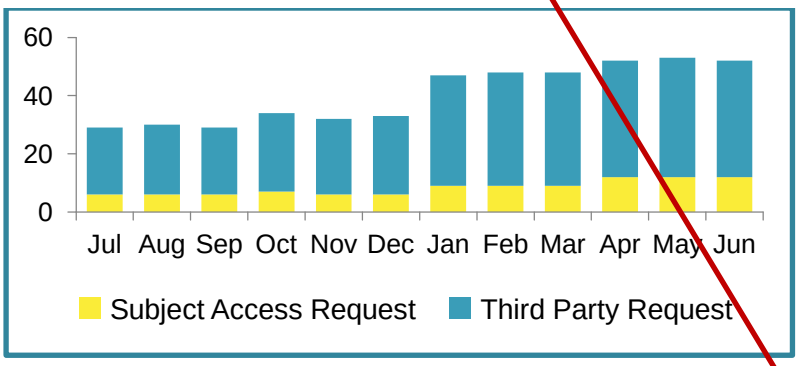
Data Protection Act 1998

Data Protection Requests

Quarterly number of requests received

Type of Request	This Quarter	Last Quarter
Subject Access Requests	36	27
Third Party Requests	121	116

Number of requests received over the last 12 months



Requests received by Directorate

Type of Request	Subject Access Request	Third Party Request	TOTAL
Aberdeen City Health and Social Care Partnership	21	45	66
Communities, Housing & Infrastructure	4	72	76
Corporate Governance	4	0	4
Educations & Children's Services	7	4	11
Office of the Chief Executive	0	0	0

Data Protection Act 1998

The Data Protection Act 1998 (DPA) regulates the Council's role, rights and responsibilities in the use, management and protection of our customers' (staff and the public) personal data.

Subject Access Requests

Anyone who we hold personal information about can ask us for a copy of it.

Third Party Requests

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

Commentary on number of requests received

The number of third party requests is up slightly since last quarter's large increase. As before the bulk of third party requests are Police requests to CH&I and government agency requests to Social Work.

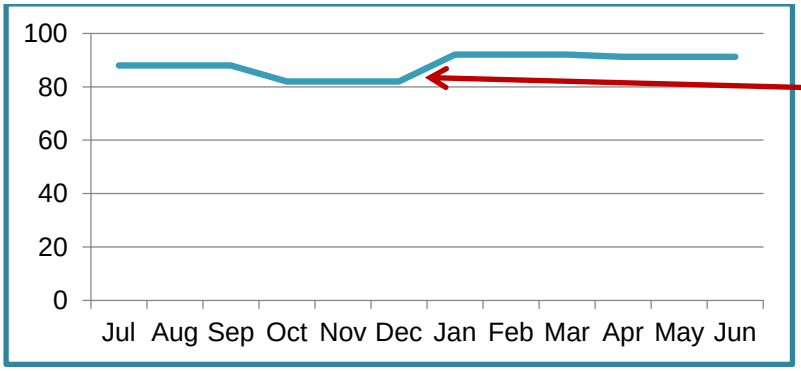
Quarterly compliance with timescales

Type of Request	This Quarter	Last Quarter
Subject Access Requests	91.24%	93%

Timescales for responding

The Council must provide the personal information requested within 40 calendar days.

Compliance with timescales over the last 12 months



Commentary on compliance

Compliance dip from Oct-Jan due to increase in volume of requests received by Education & Children's Services, who have reviewed their processes for handling requests to improve response times.

Compliance with timescales by Directorate

Directorate	On time	Late
Aberdeen City Health & Social Care Partnership	46	11
Communities, Housing & Infrastructure	75	1
Corporate Governance	2	0
Education & Children's Services	2	1
Office of the Chief Executive	0	0

Commentary on compliance by Directorate

These requests required significant staff time to examine large volumes of information requiring redaction. Highlighted potential issues with resourcing of request processing.

Breakdown of late requests by Directorate

Directorate	Request type	Response Time (days)
Aberdeen City Health and Social Care Partnership	SAR	43
	TPR	45
	SAR	49
	TPR	50
	SAR	52
	SAR	55
	TPR	80
	TPR	80
	SAR	80
	SAR	80
	SAR	96
Education & Children's Services	TPR	49
Communities, Housing & Infrastructure	SAR	42

Commentary on response times

These requests required significant staff time to examine large volumes of information requiring redaction. Highlighted potential issues with resourcing of request processing. These figures also include long-running and complex requests (four SARs and three TPRs) from a previous quarter that concluded in this one.

Data Protection Breaches and Complaints

Quarterly breaches and complaints

Breaches	This Quarter	Last Quarter
Breaches	8	12
Self-Reports to the ICO	2	1
Data Handling Complaints	1	0

Commentary on Breaches

The ICO self-reported breaches involved the accidental attachment to an email of a spreadsheet detailing details of bus lane appeals. In the course of investigating the breach, a copy of the screenshot was sent to another council employee in error. Both these incidents were lodged as separate breaches.

The Data Handling complaint was made in relation to inaccurate data contained in a Child Protection Order.

Data Protection Breaches

All breaches should be reported in line with the Council's procedures. The action taken will depend on the nature of the breach.

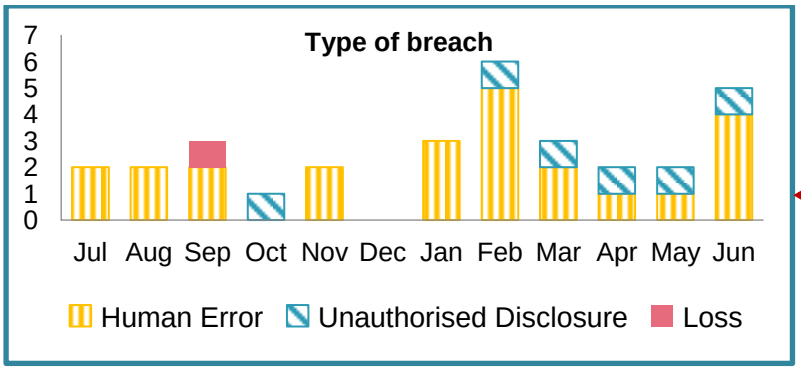
Self-Reportable Breaches

Where the nature of a breach poses significant actual or potential detriment to individuals the Council should self-report to the ICO.

Data Handling Complaints

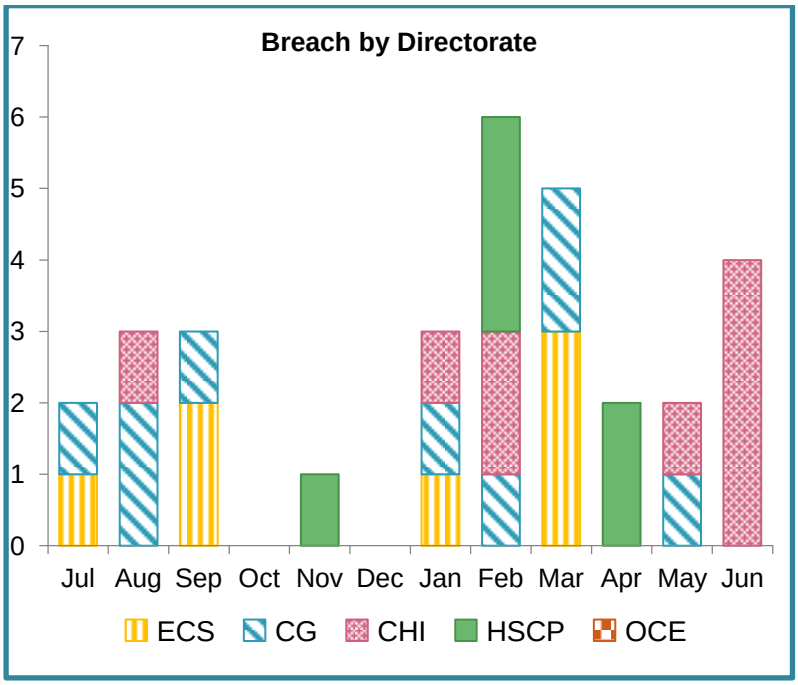
Anyone who is unhappy with the way that the Council has handled their personal data can make a complaint to us. If they are unhappy with our response to their complaint they may escalate their complaint to the ICO.

Breaches by type over the last 12 months



Commentary on type of breach

Human error remains the most common cause of data protection breaches and highlights issues around uptake of staff training and awareness included for action below.



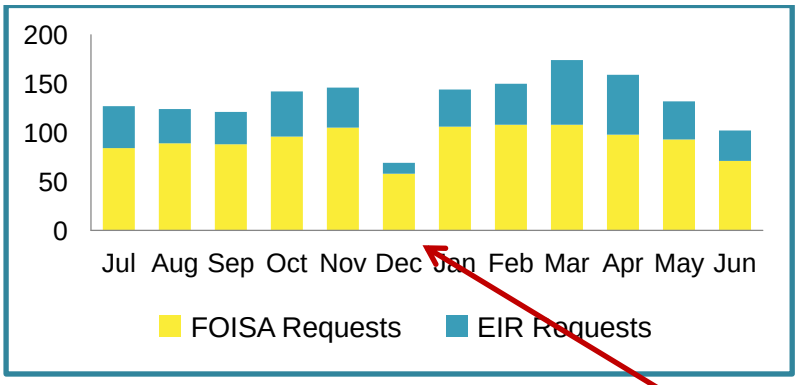
Data Protection issues for further investigation	
Investigate increase in Third Party Requests	Adapting & Learning
Resourcing of request processing	Systems & Processes
DPA Mandatory Training Compliance	People & Behaviour
Develop the processes for investigation of all breaches and subsequent remedial actions	Systems & Processes

Freedom of Information (Scotland) Act 2002 & Environmental Information (Scotland) Regulations 2004

Quarterly number of requests received

Number of requests received	This Quarter	Last Quarter
Number of FOISA Requests	262	323
Number of EIR Requests	131	145

Request numbers in the last 12 months

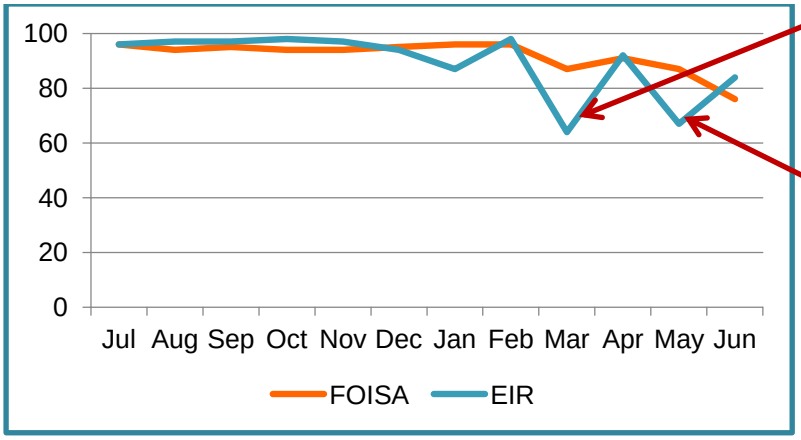


Compliance with statutory timescales

Quarterly compliance with timescales

Requests responded to within timescale	This Quarter	Last Quarter
Number of FOISA Requests	89%	93%
Number of EIR Requests	85%	96%

Compliance with timescales in the last 12 months (%)



The Freedom of Information (Scotland) Act 2002

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, with certain conditions.

Timescales for responding

The Council must respond to any request we receive within 20 working days.

Commentary on request numbers

Request numbers have remained fairly steady over the last 12 months, in line with longer terms variation across a previous years. The dip in request numbers received over the festive period is consistent with previous years.

Commentary on compliance

The dip in compliance in December relates to 4 late EIR requests, all within Communities, Housing & Infrastructure.

Potential resourcing issues around request handling and processes for handling requests will be explored.

FOISA and EIR Request Internal Reviews

Type of review received	This Quarter	Last Quarter
No response received	5	3
Unhappy with response	2	1

Type of review outcome	This Quarter	Last Quarter
Response upheld	1	1
Response overturned or amended	1	0

Internal Review

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.

Internal Review Panels

Where a requester is unhappy with our response, an internal review panel will decide whether to uphold the Council's response or to overturn or amend it.

Commentary on Internal Reviews

Upheld: relates to a request for a letter about HMO licensing information. The Council issued an 'information not held' response which was upheld as the review panel were satisfied that appropriate searches had been conducted.

Overturned: relates to a request for information about payments to celebrities. Initially some information was refused on the basis that it was personal. The review panel were satisfied that the contractual nature of the relationship between the Council and the celebrities meant that the information did not fall within the personal information exemption and could be released.

FOISA and EIR Request Appeals

No. of Appeals	This Quarter	Last Quarter
New appeals	1	1
Ongoing appeals	0	0
Closed appeals	1	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

New appeal relates to a request for a late docket for a committee report. The requester is questioning the Council's response that it no longer holds this information. Investigation underway.

Closed Appeal relates to information about Blue Badges. Requester concerned Council did not provide all the relevant information we hold. The Commissioner was satisfied that we did and our response was upheld.

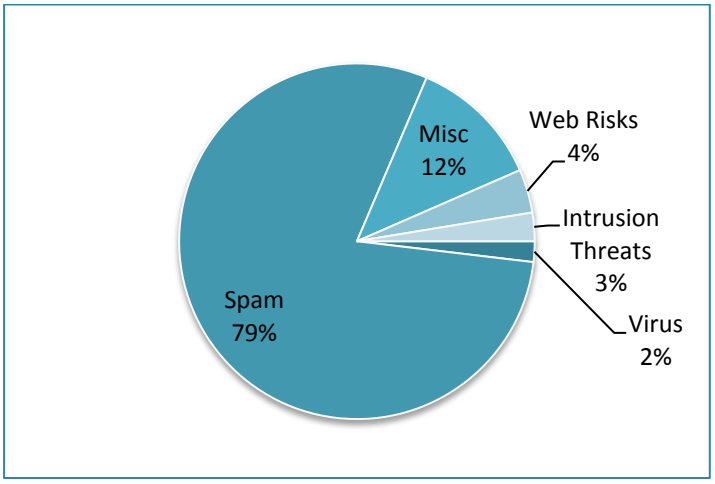
FOISA and EIR issues for further investigation	
Scope potential resourcing issues around request handling in CHI	Systems & Processes
Scope practice for evidencing retention and disposal practice	Systems & Processes
Scope potential issues at Communications approval stage	Systems & Processes

Information Security

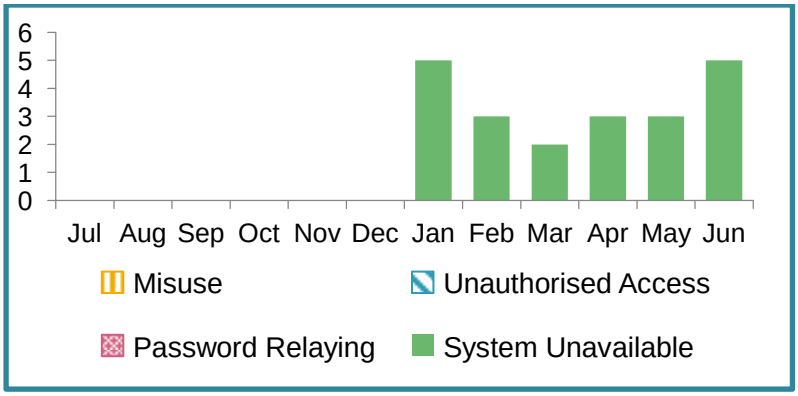
Virtual Incidents

Incident Type	This Quarter	Last Quarter
Internal Virtual Incident Attempts		
Internal Virtual Incidents	11	10
External Virtual Incident Attempts	1377001	595000
External Virtual Incidents	2	1

Breakdown: External Virtual Incident Attempts



Internal Virtual Incidents



Information Security

The Council is responsible for the integrity, confidentiality and availability of its information. The Council protects it from internal and external threats by using all available controls, and ensuring that any incident which could cause damage to the Council's assets and reputation is prevented and/or minimised.

Internal Virtual Incidents

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

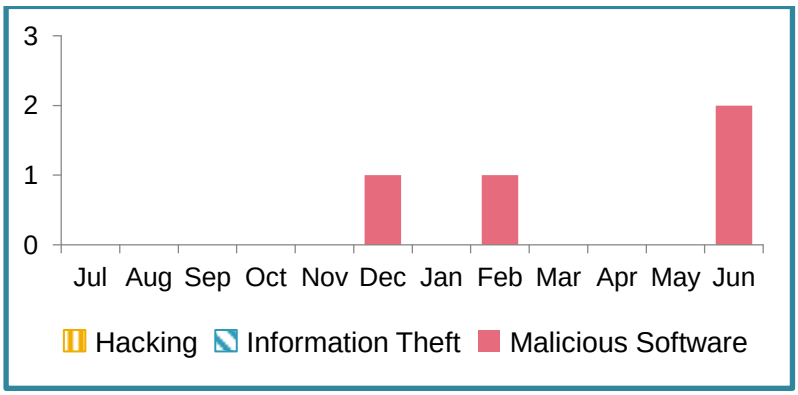
Commentary on Internal Virtual Incidents

11 occasions were recorded when business/mission critical systems were unavailable:

- 3 faulty power supplies
- 2 uncontrolled changes by system owners
- 2 phone exchange outages
- 1 supplier issue
- 1 act of vandalism
- 1 power outage
- 1 broadband contract expiry

Ongoing monitoring and investigation is being undertaken where needed.

External Virtual Incidents



External Virtual 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 Virtual Incidents

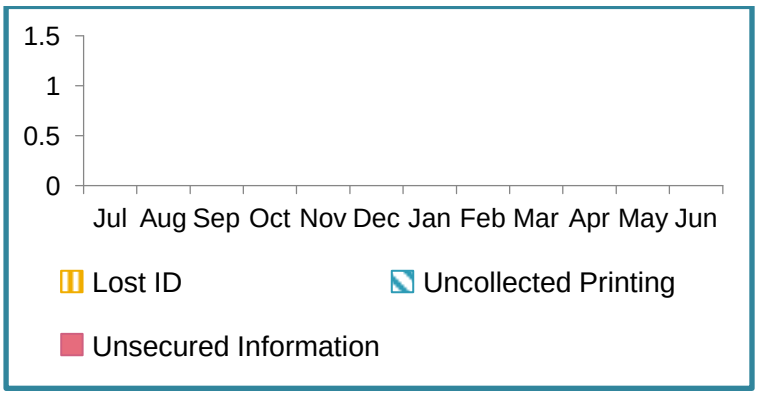
Incident attempts data from December 2015 only.

2 virus incidents were recorded in June.

Physical Incidents

Incident Type	This Quarter	Last Quarter
Internal Physical Incident Attempts		
Internal Physical Incidents		
External Physical Incident Attempts		
External Physical Incidents		

Internal Physical Incidents



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

Data collection has begun as of July 2016 and will be included in the next quarterly report.

External Physical Incidents

External Physical Incidents

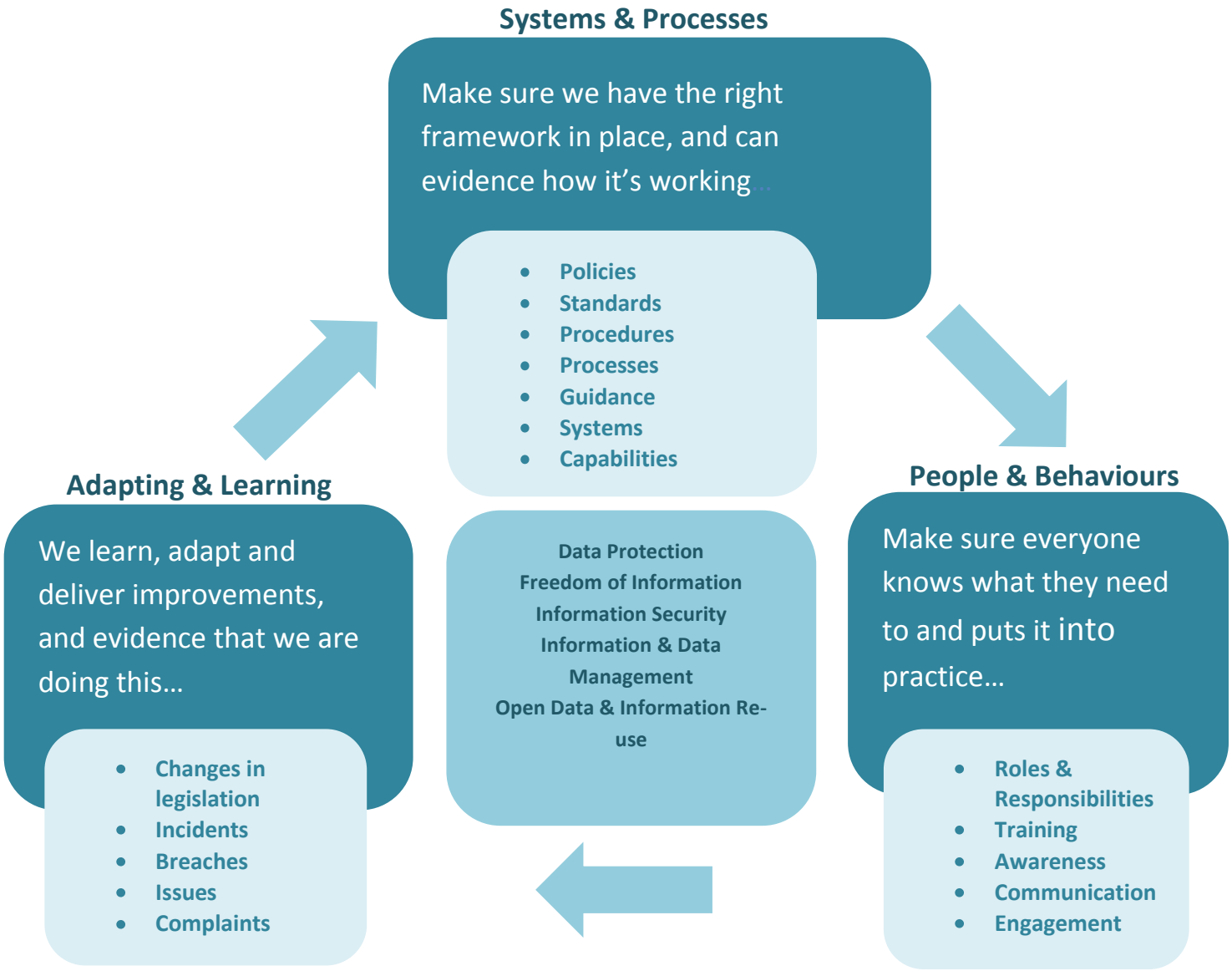
These are tangible and material risks or threats to the Council's information assets that originate from outside the premises or from the public.

Commentary on External Physical Incidents

Data collection has begun as of July 2016 and will be included in the next quarterly report.

Information Security issues for further investigation	
Investigate gaps in Change Request & Authorisation process	Systems & Processes
Investigate information sharing practices outside of network	People & Behaviours

Appendix 2: Approach



Appendix 3: Terms of Reference for the Information Governance Group

Title	Information Governance Group		
Lead	Simon Haston		
Date	June 2016	**Version**	V0.1

Purpose
The Information Governance Group's purpose is to support and drive the broader, information-governance agenda, provide the CMT with the assurance that effective control mechanisms are in place within the organisation and manage and mitigate the Council's information risks.

Meeting Frequency	**Quorum**
Monthly	Chairperson (or nominated other) and 3 others

Remit and Responsibilities
• Monitor and manage information governance assurance through the information governance framework • Manage the Council's information risk register and consider and manage emerging information issues and risks. • Report on areas or issues requiring attention or action at CMT level

Membership
Core Members ➢ Senior Information Risk Owner (Chairperson) ➢ Information Manager ➢ Public Performance Reporting & Digital Engagement Manager ➢ Performance & Risk Manager ➢ Digital Transformation Manager

- Information Security Officer
- IT Security Architect
- Legal Manager
- Information Management Team Leader
- Counter Fraud Officer
- Data Sharing Analyst, NHS

By Invitation

- Senior Officer from each Directorate
- Business Manager from each Directorate
- Any additional, relevant internal or external parties

Governance and Reporting Arrangements
• The Senior Information Risk Owner (Head of IT & Transformation) will chair the group; • The Group will be accountable to the Corporate Management Team (CMT); • Assurance in each area within scope will be reported to the Group via the corporate performance dashboard and exception report, outlining actions/decisions required from the Group; • The Group will, through the chair, report quarterly to the CMT on any areas requiring attention or action; • The Group will, through the chair, report annually on information governance to the Council's Audit, Risk & Scrutiny Committee.

Governance and Reporting Arrangements