Information Governance Management

Annual Report

Senior Information Risk Owner

July 2017-
June 2018

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 second 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 by the Information Governance Group.

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, the Information Governance Group has established an Information Assurance Improvement Plan which will implement the required medium-term assurance improvements required. The Information Assurance Improvement Plan is focussed on the following nine key assurance areas:

- Oversight & Control
- Legal & Business Requirements
- Technical & Physical Security
- Business Continuity & Disaster Recovery
- Information Sharing & Integration
- Culture, Awareness & Training
- Information Preservation
- Information for Strategic Performance Management & Transformation
- Realising Information Re-use Value

1.6 The Executive Summary at Section 2 of this report brings together the Information Governance Group's key activities from the last year; this includes activity arising from the ongoing monitoring of performance, and measures to improve assurance in the medium term.

2. Information Assurance Improvement Plan: Executive Summary of progress to June 2018

Assurance Area	Key Issues	Improvement Action Taken	Result	Key Next Steps	Value
Oversight & Control	Information Asset level assurance and monitoring arrangements and assurance required	Information Asset assurance framework developed and established	Clear framework in place of roles, responsibilities and monitoring and assurance arrangements for Council information assets	IG Group refresh to align with new Senior Information Risk Owner (SIRO) and Target Operating Model (TOM) functions will continue to monitor and report on Information Governance (IG) and to take appropriate remedial action as required Continue to report progress updates to SIRO in quarterly Information Governance Reports, with exceptions escalated to Corporate Management Team (CMT)	The Council is undertaking appropriate monitoring, and continuously improving assurance around its information and data
Legal & Business Requirements	Council requirements for changes to Data Protection law (GDPR and the Data Protection Act 2018) which became enforceable from 25 May 2018	GDPR Readiness programme rolled out to implement changes in three key areas of information & data, systems and processes, people & behaviour.	The Council has implemented measures to address changing compliance requirements	Continue to embed the foundations implemented as the Council's business as usual arrangements for the new compliance environment, folding in any actions identified by internal audit of GDPR Readiness.	The Council has the right framework in place to give assurance around its compliance with Data Protection legalisation
Technical &	The Council's firewall required updating to take advantage of	Next Generation Firewall has been implemented	The Council has up to date firewall protection in place	Tuning and further development of the solution to reach the	The Council is keeping its cyber network protection up to date

Assurance Area	Key Issues	Improvement Action Taken	Result	Key Next Steps	Value
Physical Security	advances in available solutions		Cyber Essentials Plus Certificate 2018 awarded	best operational configuration	
	The Council requires to further enhance the email solution security for external communication	Transport Layer Security (TLS) and Sender Policy Framework (SPF) implemented	Implement Secure Email Blueprint	Implement Domain-based Message Authentication Reporting and Conformance (DMARC) and Domain-Keys Identified Mail (DKIM)	The Council has appropriate security of email communication and assurance for the public
	The Council requires all applications to be risk assessed to ensure all security controls are maintained to standards, and in accordance with disaster recovery and business continuity plans	Cycle of application risk assessment programme complete	Register of risk assessment now in place and ongoing as business as usual	Further development to link application risk register to other information and data assets already in place	The council has the necessary technical and physical resilience measures in place
Information Sharing & Integration	Information Sharing (IS) guidance and protocols reviewed due to changes in data protection law	Information Sharing Protocol (ISP) Register created and maintained for recording and reporting purposes	The Council understands its current information sharing arrangements for high risk, special category business functions	Review of sharing arrangements and update agreements where required. Review and update, as appropriate, information sharing procedures, guidance and templates for changes to Data Protection law.	The Council has appropriate governance arrangements in place to continue to share information compliantly with partners in accordance with Data Protection Act 2018
Business Continuity & Disaster Recovery	The Council requires a high level of assurance around business continuity and disaster recovery arrangements for critical systems	Phase 1 complete, Phase 2 in progress	The Council understands where its business critical systems are and has improvement programme in place	Joint working with Business Continuity & Emergency Planning to make sure that appropriate arrangements are in place for resilience	The Council understands its assets and can continue to work and recover in the event of an incident

Assurance Area	Key Issues	Improvement Action Taken	Result	Key Next Steps	Value
	The Council requires an emergency on-call system for data breaches to be managed out of hours by the Duty Emergency Response coordinators (DERC)	On-call listing to incorporate Data Protection Officer advice and designated Chief Officer and Information Asset Owner	Data breaches can be responded to within the notification periods required of Data Protection Act 2018	SIRO will establish revised DERC duties accordingly	The Council has appropriate data breach management in place to assess impact and likelihood of harm following a data breach out of hours, take appropriate action and notify the Information commissioner where necessary.
Training, Culture & Awareness	Staff and members need regular and up to date Information Governance Training	New Information Governance OIL training module launched Extensive face to face sessions delivered to staff in key roles as part of GDPR Readiness activities	Mandatory Information Governance online training in place for all staff 1200 staff in key roles attended face to face training as part of GDPR readiness activities	Monitor the uptake of mandatory OIL training through monthly exception reporting Continue to develop and deliver targeted face to face training based on staff roles	Our Staff have the right knowledge to play their role in the appropriate use and governance of the Council's information and data
	Providing appropriate support to ALEOs and partners	Guidance and support for Community Councils developed and shared ALEO GDPR Information sessions developed and delivered	Data Protection guidance and templates in place for Community Councils 3 Information Sessions for ALEOs delivered in Feb 2018.	Establish IG practice sharing and support Forum with ALEOs	The Council is establishing the right relationships and supports to promote and support good IG practice amongst our wider family.
Information Preservation	Ensuring that where appropriate key Council records are preserved	The Archives Service develop a preservation forum with Information Asset Owners (3rd Tier managers) to ensure the appropriate transfer of all records requiring preservation is in place	The archives service develop a transfer preservation roadmap for records aligned to TOM business functions and Information Asset owners	Information Preservation transfer Register is established and maintained	The Council retains all identified and necessary business records that provide the corporate memory of its people across the place of Aberdeen

Assurance Area	Key Issues	Improvement Action Taken	Result	Key Next Steps	Value
Strategic Performance Management & Transformation	The Council has a fragmented understanding of its customers because of lack of data integration between key systems	Master Data Management Hub and Integration layer business requirements developed. Logical Data model developed	The Council is ready to procure a Master Data Management Hub and Integration layer	Procurement and implementation of Master Data Management Hub and Integration layer	The Council has the capability required to integrate its data about people and place
Realising Information Re-use Value	The Council wants to leverage the value of its information to be a data-driven, evidence-based decision making organisation	Two Business Intelligence pilots to be run, testing the governance requirements and analytics capabilities possible	The Council has an understanding of analytics capabilities from existing data sources that inform business intelligence technologies required	Test and evaluate business intelligence pilots	The Council has real-time insights and intelligence about service demand, resource allocation with predictive capabilities at individual, service and functional levels
	The Council wants to open up its non-personal data wherever possible to the benefit of its people, economy and place	Open Data Standards have been developed as part of the National Open Data Programme the Council is a part of. The Council has established its place within the Scottish Cities Alliance to publish core open data across local authority consortium	The Council is working collaboratively to build the foundations required for a sustainable open data programme	Open Data Platform to be implemented and regular open data publishing schedule to be agreed	The Council is opening up its data to benefit the people, place and economy of Aberdeen

3. Information Governance Performance Information July 2016- June 2017

3.1 Data Protection Requests

Fig.1: Annual number of requests received

Type of Request	12 months to June 2018	12 months to June 2017
Subject Access Requests	184	144
Third Party Requests	509	604

Fig. 2: Requests received in the 12 months to June 2018

Fig. 3: Requests received by Directorate (Jul 2017 – Mar 2018)

Directorate	Subject Access Request	Third Party Request	TOTAL
Aberdeen City Health & Social Care Partnership	12	29	41
Communities, Housing & Infrastructure	38	193	231
Corporate Governance	16	32	48
Education & Children's Services	46	71	117
Office of the Chief Executive	0	0	0
Joint H&SCP E&CS	19	57	76

Data Protection Requests

Data Protection legislation 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 data 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

In the last 12 months there has been an increase in SARs and a decline in reported TPRs.

The highest levels of SARs and TPRs were received for the areas of Customer (Early Intervention and Community Empowerment and Housing) and Operations (Integrated Children & Family Services). These requests are highest in the usual service areas however their management now falls within the Customer Function (see Fig. 4).

Of the 509 TPRs received in the last 12 months, 210 were related to CCTV.

Fig. 4: Requests received by Function (Apr 2018 – Jun 2018)

Function	Subject Access Request	Third Party Request	TOTAL
Commissioning	0	0	0
Customer	42	127	169
Operations	Data Protection Requests for Operations are managed by the Customer Function		
Resources	3	0	3
Governance	1	0	1
Place	7	0	7

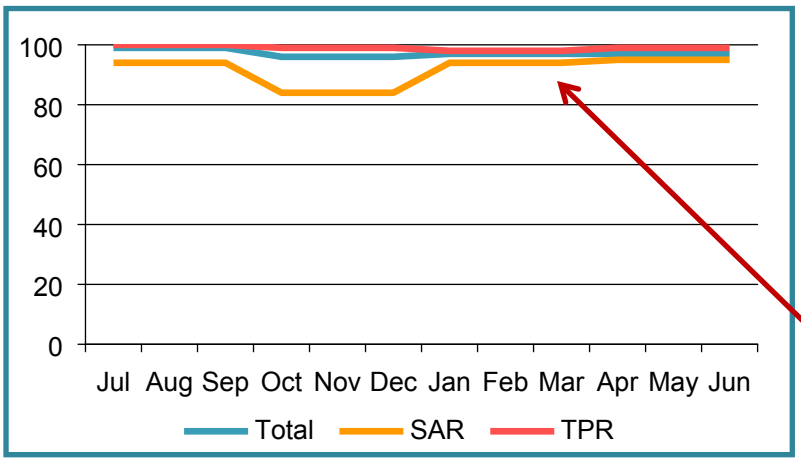
Fig. 5: Breakdown of requests received by Customer Function (Apr 2018 – Jun 2018)

Service Area	Subject Access Request	Third Party Request	TOTAL
Children's Social Work	28	13	41
Adults Social Work	4	2	6
Joint Children's and Adults Social Work	0	5	5
Education	4	0	4
Revenues & Benefits	0	9	9
Housing	6	36	42
Early Intervention and Community Empowerment	0	62	62

Fig. 6: Corporate compliance with timescales for requests

Type of Request	12 months to June 2018	12 months to June 2017
Subject Access Requests	92%	68%
Third Party Requests	99%	97%
Total compliance	97%	91%

Fig. 7: Corporate compliance with timescales over the last 12 months



Timescales for responding

Until the 25th May the Council had 40 calendar days to provide the personal information requested in response to data protection requests. Since the 25th May (following GDPR being enacted), the timescale is now reduced to 30 days.

If a request involves a large and complex set of information, the timescale can be extended for a further 2 months, if the customer is notified of this within the first month.

Commentary on compliance

Compliance with timescales for SARs and TPRs has been consistent over the past 12 months with an increase of 5% overall on last year. Compliance rates have improved in each category.

The majority of Data Protection requests are TPRs which tend to be for limited information which can be delivered quickly. SARs for social care records often involve reviewing and redacting large and complex case files.

3.2 Data Protection Breaches and Complaints

Fig. 8: Annual breaches and data handling complaints

Breaches	12 months to June 2018	12 months to June 2017
Breaches	61	35
Self-Reports to the ICO	1	0
Data Handling Complaints	4	0

Fig. 9: Breaches by type over the last 12 months

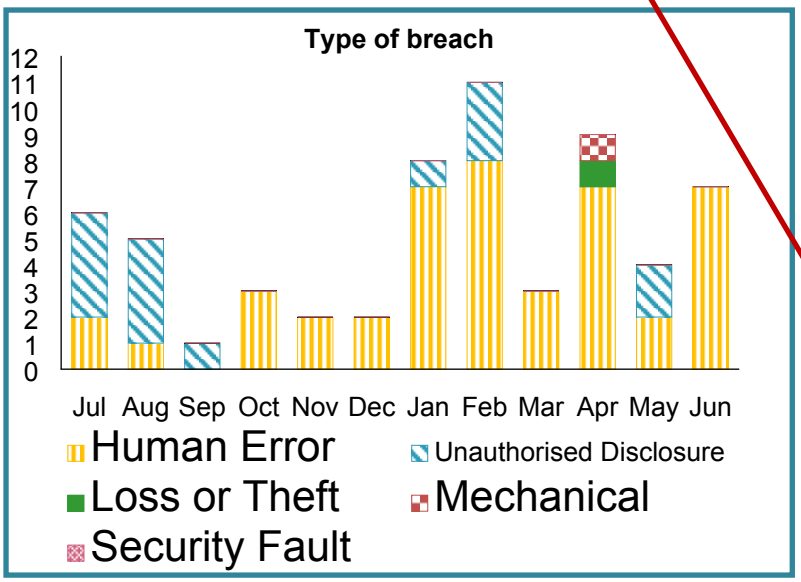
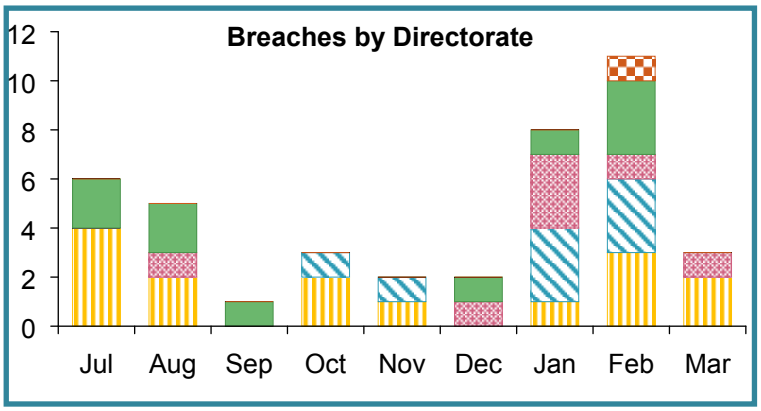


Fig. 10: Breaches by Directorate Jul 2017 – Mar 2018



Data Protection Breaches

All potential 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.

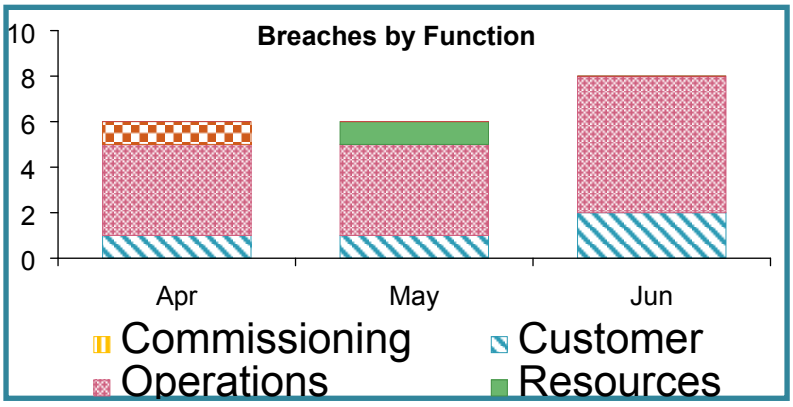
Data Handling Complaints

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.

Commentary on number and type of breaches

There has been a significant increase in the number of breaches reported in the last 12 months. The increase has been concentrated in the last 2 quarters. This is likely due to increased awareness through a significant increase in GDPR training implemented during the year and the recognised need to report breaches quickly under the new Data Protection Act 2018.

Fig. 11: Breaches by Function Apr 2018 – June 2018



Commentary on breaches by Function

Almost three quarters of reported breaches (14) originated in the Operations Function of the Council in Integrated Children & Family Services or Adult Social Care in the Health & Social Care Partnership.

Fig. 12: Breaches self-reported to the ICO this year

When breach occurred	Breach Type	Breach Description	No. Of data subjects impacted	ICO Breach reporting compliance (72hrs)	Remedial Actions
June 2018	Loss or Theft	Missing holdall	1	✓	i) The Council has pursued action with the third-party ii) The Service have revised their procedures and protocols for the secure transfer of items
July 2018	Human Error	Misdirected P11D Tax Forms	947	✓	i) The Council has contacted all affected individuals to inform them of the breach and apologise iii) Revised procedures with additional quality assurance

3.3 Data Protection Advice & Support

Fig. 13: Number of requests received (25th May - 30th June 2018)

Number of requests received	25th May – end of June
Internal enquiries	75
External enquiries (from the public or other organisations)	15

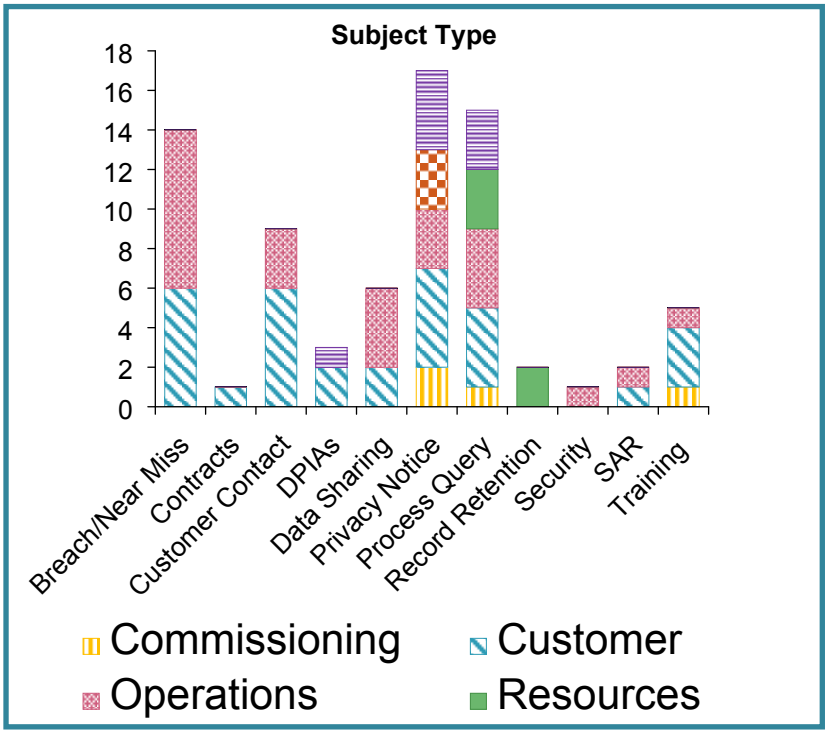
Data Protection Officer

Since the 25th May the Council has been required to have a statutory Data Protection Officer (DPO). The Council's DPO is Fraser Bell, Chief Officer, Governance.

Data Protection Queries and Complaints

Monitoring and responding to DPO enquiries has been delegated to officers in the Governance, Legal and Information and Data Governance Office

Fig. 14: Breakdown of internal enquiries to the DPO by Subject Type and by Council Function, (25th May - 30th June 2018)



Commentary on internal DPO enquiries

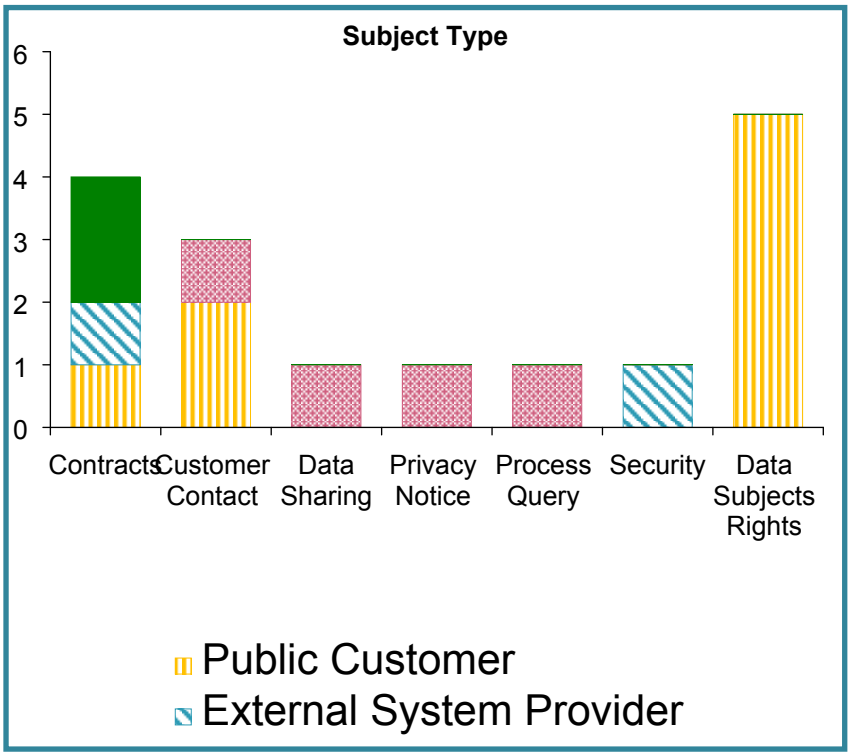
The highest number of enquiries this quarter related to supporting Information Asset Owners to draft and implement privacy notices to inform data subjects about how their data is being used under the 2018 Act.

Process queries from staff asking questions about practice under the new legislation were the second highest category of request, also aligned to bedding in changes required by GDPR.

Reports of data breaches or near misses were the third highest category of request. Breaches are outlined in more detail in the section above (Figs. 9 and 10).

New mandatory DP and IG training generated additional demand for more support, guidance and advice.

Fig. 15: Breakdown of external enquiries to the DPO by Subject Type (25th May - 30th June 2018)



Commentary on external DPO enquiries

The highest number of public enquiries received immediately after GDPR came into force related to Data Subject's rights under the 2018 Act.

Subject Access Requests or Third Party Requests received and passed onto the appropriate services are not counted in these statistics as they are counted in the section above on Data Protection Requests.

The Council also received a number of requests from other organisations asking for advice, guidance and support about (GDPR) Data Protection Act 2018 compliance.

3. 4 Information Governance Training

Over the past 12 months the Council's (GDPR Readiness) Data Protection Act 2018 Activities were built around the following key areas:

- Information & Data
- Systems & Processes
- People & Behaviour

Within the People & Behaviour area, a programme of reporting, guidance, training & briefing sessions, workshops and any additional targeted support required for services has been provided. This was targeted as follows:

Fig.16: Training sessions for Senior Managers (Information Asset Owners)

Session Name	Attendees at sessions
Information Asset Owner Session 1	Attended by 96% of the Council's Information Asset Owners, currently just over 100 in number
Information Asset Owner Session 2	
Third Tier Network & ECMT	

Commentary on training and guidance for Information Asset Owners

The Council's Information Asset Owners are third-tier managers who are responsible and accountable to the Council's Senior Information Risk Owner (SIRO) for the specific, defined information assets within their remit. Their role and responsibilities are set out the Council's Information Asset Owner Handbook, which includes required actions around readiness for changes to Data Protection Law.

A two-part training session on the Information Asset Owner Role and Changes to Data Protection Law and was delivered to Information Asset Owners from September 2017 – November 2017. These sessions had follow up actions for all Information Asset Owners to take in relation to their information assets in order to be ready for changes to data protection law. This was followed up with further sessions for staff within their services and with targeted intensive support to complete the required actions.

A further presentation on Changes to Data Protection Law was given was given to all the Council's Information Asset Owners and Chief Officers on 12 December 2018 to check in on progress with agreed actions.

Fig.17: Further training sessions by category of attendee

Session	Sessions	Attendees at sessions
Information Asset / Data Stewards	7	55
Elected Members	5	30
Open to all staff	10	82

Commentary on further training and guidance for other categories of attendees

In addition to the formal training sessions, services were provided with a range of intensive support and guidance by the Council's Information Governance & Legal Teams through briefings at management teams, workshops and meetings and one-to one sessions to complete required readiness actions.

Fig.18: Training sessions for staff processing special category, high risk, personal data

Function/Cluster	Sessions	Attendees at sessions
Aberdeen City Health & Social Care Partnership	10	320
Children's Social Work	11	257
Revenues & Benefits	2	87
Communities & Housing	4	113
Customer Services	11	58

Commentary on training for staff in high risk business areas

Sessions were delivered to high risk business areas. These sessions were designed to address the specific knowledge and understanding needs of the particular staff groups.

Business areas are deemed high risk if staff are likely to work with special category data and/or are front line staff working directly with customers.

Fig 19: Information Governance online training

Function	% of workforce who have completed training, as 12 noon, 11 September 2018
Adult Social Work (Aberdeen City Health & Social Care Partnership)	47%
Commissioning	78%
Customer	83%
Governance	96%
Operations	34%
City Growth	37%
Strategic Place Planning	70%
Resources	71%

Commentary on mandatory information governance training

Mandatory training went live in July 2018. There has been a steady increase in uptake, due to the time of year and the amount of staff on annual.

Exception reporting will be provided to the leadership team on monthly basis to ensure compliance.

By the end of September all staff will have completed the mandatory training.

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

3.5.1 FOISA and EIR Information Requests

Fig 20: Annual number of requests received in the period

Number of requests received	12 months to June 2018	12 months to June 2017
Number of FOISA Requests	1348	1335
Number of EIR Requests	636	466

Fig 21: Request numbers in the last 12 months

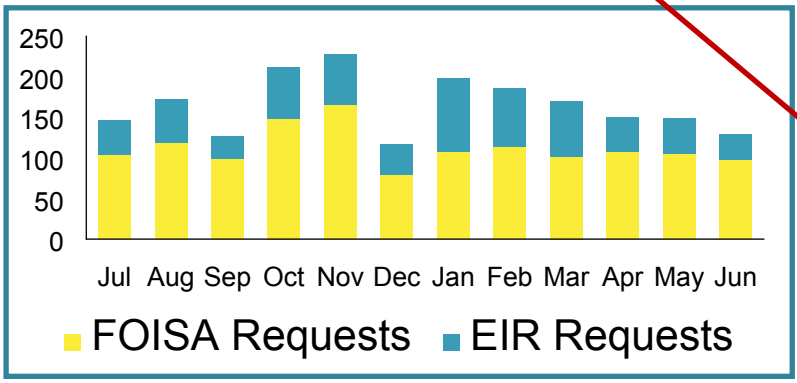
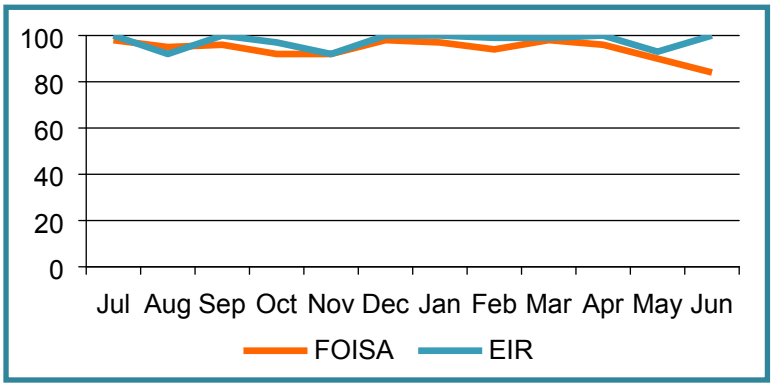


Fig 22: Compliance with timescales in the period

Requests responded to within timescale	12 months to June 2018	12 months to June 2017
FOISA Requests	94%	93%
EIR Requests	98%	95%

Fig 23: Compliance with timescales 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 request numbers

There has been a 10% increase in FOISA and EIR information requests as a whole over the past 12 months. This increase is related to greater awareness of staff in recognising FOISA and EIR requests which has resulted in better recording and reporting. The increase is also related to high profile news stories which generate public interest.

Commentary on compliance

Compliance rates for FOISA and EIR requests have increased this year, compared with last year, despite the increasing numbers received.

3.5.2 FOISA and EIR Request Internal Reviews

Fig. 24: Internal Reviews received by type in the period

Type of review received	12 months to June 2018	12 months to June 2017
No response received	10	6
Unhappy with response	39	20

Fig.25: Internal Review Panel outcomes in the period

Type of review outcome	12 months to June 2018	12 months to June 2017
Response upheld	32	14
Response overturned or amended	17	9

3.5.3 FOISA and EIR Request Appeals

Fig. 26: FOISA and EIR Appeals received and closed in the period

No. of Appeals	12 months to June 2018	12 months to June 2017
Received	3	8
Closed	4	7

Fig. 27: FOISA and EIR Appeal outcomes in the period

Appeal Outcomes	12 months to June 2018	12 months to June 2017
Council response upheld	3	3
Council response partially upheld	1	0
Lateness	0	1
Council response overturned	0	3

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.

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.

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 Council received less appeals this year than last year. Of the appeal outcomes in the period no responses have been overturned, three responses have been upheld and one was partially upheld.

3.6 Information Preservation: Historical Archive

Accessions

Fig. 28: Annual number of Accessions received (excluding non-City accessions)

Number of City Accessions	12 months to June 2018	12 months to June 2017
Total	272	308
Received from internal departments	262	283
Aligned to retention schedule	261	275
Received in electronic form	0	10

Fig. 29: Annual number of accessions received

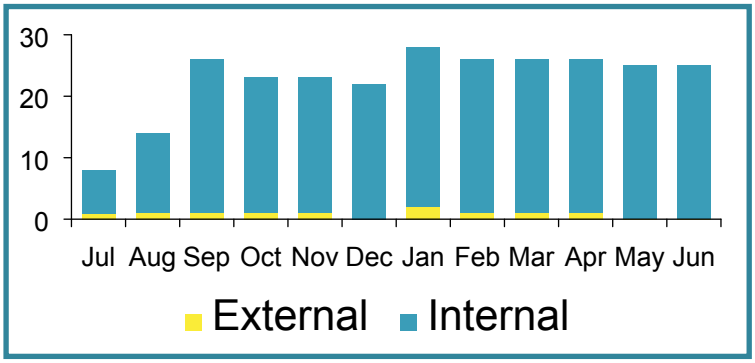


Fig. 30: Accessions received by Directorate

Directorate	Records received (Y/N)?	Description	Total
Aberdeen City Health and Social Care Partnership	N		0
Communities, Housing & Infrastructure	Y	Plans and building warrants	2
Corporate Governance	Y	Council meeting agenda papers and minutes	182
Educations & Children's Services	Y	Schools admission registers,	3

The Public Records (Scotland) Act, 2011 (PRSA)

The Public Records (Scotland) Act, 2011 (PRSA) requires the Council to make proper arrangements for its records, including the transfer of those records identified for permanent preservation to the Archives Service (Aberdeen City & Aberdeenshire Archive Service).

Transferring Records to Archives

The Council's Records Retention & Disposal Schedule (RR&DS) states that records must be offered to the Archives for review or transferred routinely to the Archives for permanent preservation.

Failure to do so has a range of consequences affecting the Council in areas such as business continuity, legislative compliance, and its reputation.

Accessions

Accessions are items and collections donated / transferred by external depositors (e.g. members of the public) and internal Council departments into the Archive collections for permanent preservation.

Commentary on Accessions

In the past year the vast majority of internal accessions have come from Democratic Services, with small numbers of accessions coming from Planning and Education. None of these deposits have been in electronic format.

		school log book, leavers registers, daily registers	
Office of the Chief Executive	N		0
Commissioning	N		0
Customer	N		0
Operations	N		0
Resources	N		0
Governance	Y	Council meeting agenda papers and minutes	75
Place	N		0

3.6.1 City Archive Enquiries (excluding Data Protection enquiries)

Fig. 31: Annual number of Enquiries received

Number of Enquiries received	12 months to June 2018	12 months to June 2017
External Enquiries	513	758 enquiries were received
Internal Enquiries	136	
Total	649	

Archival Enquiries

The Archive Service supports the work of the Council and provides public access to the records it cares for.

As part of this service it answers internal enquiries and enquiries from the public.

Fig. 32: Internal Enquiries received by Directorate

Directorate	12 months to June 2018	12 months to June 2017
Aberdeen City Health and Social Care Partnership	0	
Communities, Housing & Infrastructure	9	
Corporate Governance	15	
Educations & Children's Services	7	
Office of the Chief Executive	2	

Commentary on Enquiries received

There has been little change in the number of enquiries in the last year.

Commissioning	0	Not applicable
Customer	5	Not applicable
Operations	18	Not applicable
Resources	0	Not applicable
Governance	8	Not applicable
Place	2	Not applicable

3.7 Information Security

3.7.1 Cyber Incidents

Fig. 33: Overview of cyber incidents in the period

Incident Type	12 months to June 2018	12 months to June 2017
Internal Cyber Incident Attempts Prevented	2	1
Internal Cyber Incidents	3	6
External Cyber Incident Attempts Prevented	40790746	18089194
External Cyber Incidents	12	5

Fig. 34: Internal Cyber Incidents in the period

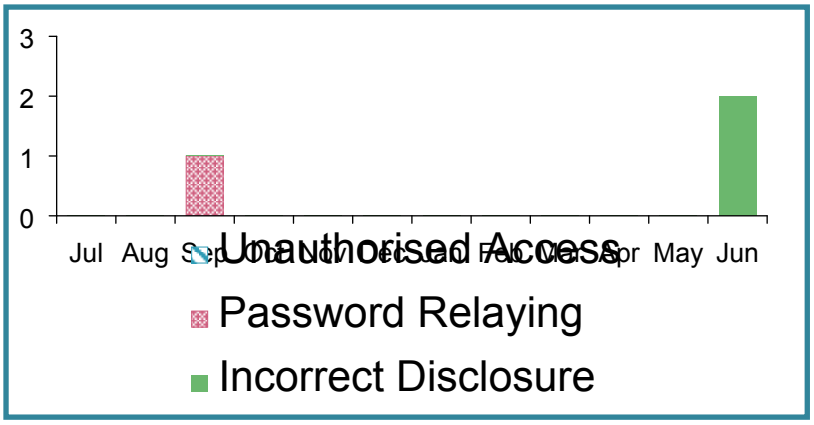
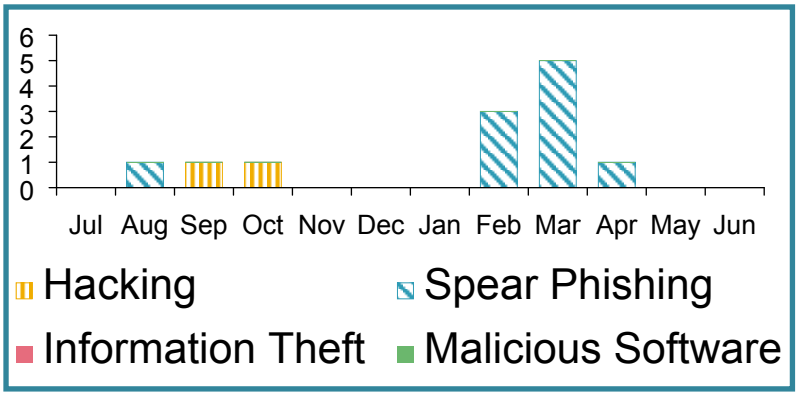


Fig. 35: External Cyber Incidents in the period



Information Security in brief

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 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.

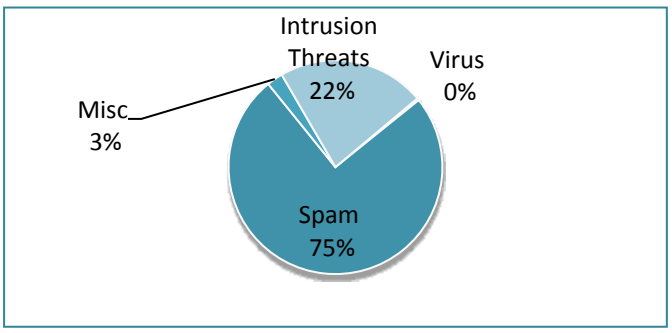
Commentary on Internal Cyber Incidents

In September an internal cyber incident occurred due to proper procedure not being followed for legitimate access to an employee's device (password relaying). There was no unauthorised access to information as a result of the incident. There were 2 instances in June in which emails were sent to internal employees disclosing information which should not have been shared.

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. 36: Breakdown of External Cyber Incident Attempts



3.7.2 Physical Incidents

Fig. 37: Physical Incidents in the period

Incident Type	12 months to June 2018	12 months to June 2017
Internal Physical Incidents	153	121
External Physical Incidents	72	74

Fig. 38: Internal Physical Incidents by type in the period

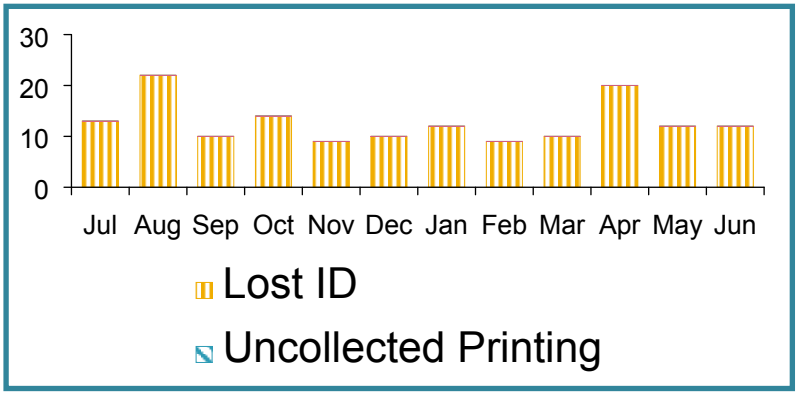
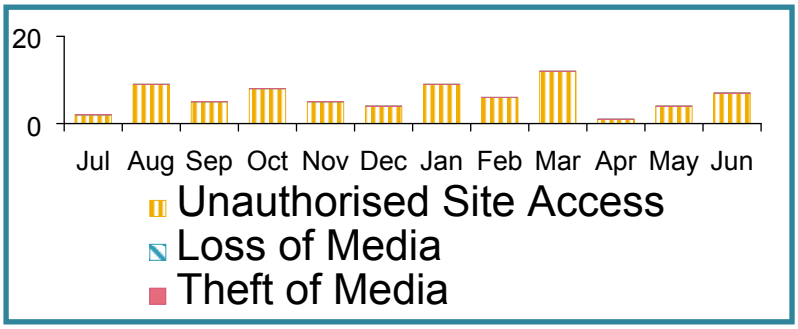


Fig 39: External Physical Incidents by type in the period



Commentary on External Cyber Incident Attempts and Incidents

The majority of external cyber incidents (10 out of 12) were successful phishing attempts. In each case the risks were mitigated.

The number of external cyber incident attempts rose by 125% in the past 12 months. 75% of these were Spam attempts.

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

There has been an increase 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 these instances is collected via Health & Safety reporting.