Annual Report: Information Governance 2023-2024

Corporate Governance & Audit Committee
September 2024

Annual Report: Information Governance 2023-2024

Statutory compliance

FOI & EIR

- Combined figures for FOI & EIR
- Information requests must be responded to within 20 working days, services required to provide the information within 15 working days to the IG Team
- Requestors can request a review; the council have a further 20 working days to respond
- In exceptional circumstances, 40 days may be allowed

Requests	2020/21	2021/22	2022/23	2023/24
Requests	1229	1308	1245	**1680**
Compliance	84%	74%	71%	**79%**
On previous year	+318 +21%	+79 +6%	-63 -%5	**+435** **+35%**

Reviews	2020/21	2021/22	2022/23	2023/24
Requests	40	75	45	**40**
Compliance	55%	66%	87%	**83%**
On previous year	+13 +48%	+35 +88%	-30 -40%	**-5** **-11%**

Analysis

- Significant increase in the number of requests on last year
- Compliance for FOI response has increased despite significant increase in numbers.
- Reducing time allowed for services to respond to 15 days has worked, some services still struggling to meet demand.
- Slight reduction in the number of requests for review. Compliance reduced slightly.

Next Steps

- Development of an FOI/EIR action plan to improve overall compliance to 95%
- Continue to work with services where demand is high/struggling to meet timescales & exploring potential solutions
- Improved communications and training for staff
- Reviewing requests and actively publishing information requested regularly

Annual Report: Information Governance 2023-2024

Statutory compliance

Subject Access Requests

- Requests for personal information about themselves
- Working with the ICO from July 22 due to delay in responding to requests and complaints
- Requests must be responded to within a calendar month, or 3 months for complex requests
- Backlog cases are those which are queued for response due to known capacity issues – will extend beyond statutory timescales.

SARs	2020/21	2021/22	2022/23	2023/24
Requests	299	279	345	**434**
No. of which are complex	23	24	20	**25**
Compliance	68%	67%	66%	**63%**
On previous year	+6 +2%	-20 -7%	+66 +24%	**+89** **+26%**

SAR Backlog 23/24	Mar	May	Jul	Aug	Oct	Dec	Feb	Apr
Requests on backlog	43	41	38	43	55	67	63	60
No. of which are complex	22	21	20	23	29	33	31	27
No. closed since last report	11	12	16	10	4	6	15	16

Analysis

- Significant increase in the number of requests on last year
- Compliance has remained relatively consistent despite increase in demand
- No pattern to receiving complex/backlog requests
- Time consuming to prepare information for release

Next steps

- Review the management of backlog cases to remove the backlog
- Continue liaising with the ICO in relation to the management of the SARs backlog
- Work with services to enhance their redaction skills to improve compliance

Annual Report: Information Governance 2023-2024

Statutory compliance

Data Subjects Rights & Disclosure Requests

- 7/8 Data subjects' rights (DSR) requests (excluding SARs)
- DSR requests must be responded to within a calendar month, or 3 months for complex requests
- Disclosure requests are personal data requests made by Police, Solicitors etc. for a specified purpose (no statutory timescale to respond but work to the same deadline as the statutory requests)

DSR Requests	2020/21	2021/22	2022/23	2023/24
Requests	48	52	69	**93**
Compliance	68%	78%	87%	**86%**
On previous year	+2 +4%	+4 +8%	+17 +33%	**+24** **+35%**

Disclosures	2020/21	2021/22	2022/23	2023/24
Requests	537	565	446	**436**
Compliance	70%	88%	85%	**79%**
On previous year	+117 +28%	+28 +5%	-119 -21%	**-10** **-2%**

Analysis

- Increase in the number of DSR requests, decrease in disclosure requests
- Compliance remains consistent for statutory obligations, slight decrease in disclosures
- Majority erasure requests following increased comms

Next steps

- Aim to build compliance year on year with an aim to achieve 95% compliance in all areas
- Review of case management processes to improve compliance on statutory requests

Annual Report: Information Governance 2023-2024

Statutory compliance - quarterly overview

FOI / EIR	Q1	Q2	Q3	Q4
2022/23	337	277	299	332
2023/24	364	427	410	477
Difference	+27	+150	+111	+145

DS Rights	Q1	Q2	Q3	Q4
2022/23	15	19	12	23
2023/24	11	19	12	51
Difference	-4	0	0	+28

SARs	Q1	Q2	Q3	Q4
2022/23	65	83	89	108
2023/24	121	107	93	113
Difference	+56	+24	+4	+5

Disclosures	Q1	Q2	Q3	Q4
2022/23	116	120	103	107
2023/24	110	127	82	117
Difference	-6	+7	-21	+10

Annual Report: Information Governance 2023-2024

Statutory compliance

Data Protection Impact Assessments (DPIA)

- DPIAs are required for processing activity containing personal data
- A DPIA is a risk assessment for data protection & privacy
- Supports privacy by design & default approach
- DPIA process currently under review & redevelopment

DPIAs	2020/21	2021/22	2022/23	2023/24
Submitted	76	76	71	73

Analysis

- DPIA submissions are consistent year on year
- DPIA process has being reviewed and a new process will be launched in summer 2024 – aimed to improve user experience
- Figures don't account for the complexity of DPIAs and associated work (data sharing agreements, privacy notices etc.)

Next steps

- Launch of the new DPIA process and associated guidance
- Comms & training for staff on DPIA completion and IAOs on sign off and risk
- Organisational & cultural change to promote risk-based approach

Information Security Incidents

- Incidents to be reported as soon as a person/service becomes aware
- IG Team determine severity of incident and advise services on appropriate next steps
- Serious incidents to be reported to the ICO within 72hrs
- Council operates a 'no blame' culture for incident reporting

Incidents	2020/21	2021/22	2022/23	2023/24
Reported total	253	289	318	**322**
Reported to ICO	1	3	6	**1**
On previous year	-32 -11%	+36 +14%	+29 +10%	**+4** **+1%**

Analysis

- Steady increase in the number of reported incidents is generally positive as it shows that colleagues are aware of the process and seek the support available
- One incident reported to ICO – no further action taken

Next steps

- Analysis of reported incidents to improve training, comms and guidance
- Improve awareness around reporting integrity and availability incidents and those data breaches not containing personal data
- Campaign to encourage incident reporting and awareness of incidents
- Improve the sharing of lessons learned to mitigate against reoccurrence

Annual Report: Information Governance 2023-2024

Mandatory training compliance

Mandatory training

- IG mandatory training is to be undertaken annually
- 95% of staff are required to have completed the training to meet the required standard
- Modules became available to staff in July 2023, some modules will be rotated this summer for additional awareness

Modules

- Five mandatory modules
    1. Introduction to Information Security
    2. UK GDPR - Why it matters
    3. Handling Sensitive Information
    4. Tutorial: UK GDPR - How does it affect individuals
    5. Tutorial: Freedom of Information

- 10 additional modules
    1. Encouraging a secure culture
    2. GDPR – Social engineering
    3. GDPR for the dispersed workforce
    4. Out of office
    5. Password security
    6. Phishing: don't take the bait
    7. Scenario: Handle with care
    8. Social media and privacy
    9. Tutorial: assessing your risk
    10. UK GDPR: How does it affect organisation

2023/24	October	January	April	June*
Completed	2,209	2,729	3,431	3,962
Not attempted	5,680	5,219	4,456	3,784
Compliance	28%	34%	44%	51%

Analysis

- Uptake in mandatory training is rising
- Above figures do not account for staff unable to complete this training e.g. dispersed workforce
- Figures do not account for in person delivered training by the IG Team
- Change in organisational culture needed to embed mandatory training uptake
- Increased communications and awareness throughout year

Annual Report: Information Governance 2023-2024

Organisational understanding

Record of Processing Activity

- Statutory requirement to document an organisations processing activities
- Acts as an inventory of the data processed, providing a clear picture of how PID is processed and whether it is compliant with applicable legislation
- It presents key information from DPIAs, data flow maps and other documentation such as contracts and sharing agreements in one central place
- A successful RoPA will enable streamlined data processing and effective information risk management
- Work ongoing in this area

DPIAs & IRM

- DPIAs are a risk assessment carried out when processing personal data
- Risks identified as part of this process should be recorded against the Information Asset (IA) on the IA Register (IAR)
- As part of the Information Risk Management (IRM) process, risks should be escalated to appropriate risk registers as required

IAR & Data flow mapping

- Outlines what information is held, where it is held & what it is used for
- IAR is in place, but further work needs to be done to embed this and progress to BAU
- Data flow mapping is to ensure that data is being shared fairly and lawfully
- Current IAR is set to be reviewed before being developed further

Contracts & Sharing Agreements

- IG Team have started to collate a record of any ISA's that we are asked to review
- Services should request advice and support from the IG Team when developing an ISA
- As part of the review for the development of the RoPA, contracts will also need to be examined to help identify information assets for the IAR.

Next steps

- Following the pilot, launch the revised DPIA process and associated guidance
- Conduct an exercise to capture required information to support the development of the RoPA and information asset register
- Development and roll out of communications, training and guidance materials for colleagues around RoPA, IAR, IRM & DPIAs
- Ensure that IAOs are clearly identified and understand their role
- Work with Risk colleagues to ensure that IRM is aligned to corporate risk reporting and appetite

Annual Report: Information Governance 2023-2024

Successes, challenges & next steps

Successes
- Implementation of new redaction software
- Installation of a new scanner
- Updated policies
- Maintaining statutory compliance rates
- Ways of working / efficiency savings
- DPIA pilot
- Communications and engagement
- Changes to IG Team operations to improve efficiency

Challenges
- Resource
- Statutory compliance
- SARs backlog
- Significant increases in demand
- Mandatory training compliance
- Support from / conflicting demand on other services
- ICO engagement
- Organisational understanding of information governance

Next steps - 2024/2025
- Continue to work on the SARs backlog with the aim of reducing the number of complex cases outstanding
- Continue to examine the effective use of resources within the IG Team to improve compliance, better support services & improve efficiencies
- Work closer with linked services (Data / IT / Legal / Contracting / Risk & Audit) to develop a strategic co-ordinated approach & support offer
- Continue work to review and refresh IG related policies and develop accompanying procedures to assist colleagues with compliance
- Revised RoPA development and roll out
- Support services & Councillors to support themselves by offering further specialist training & guidance
- Continue to raise awareness through communications channels and training around IG related issues
- Monitor revisions to data protection legislation and respond as required