Council
27 May 2021
Agenda item:17
Report no: 29/2021

Title of report	Annual Information Governance Report
Public/confidential	Public
Action	For information
Summary/purpose of report	To provide the Council with an update on the organisation's performance in complying with its obligations under the data protection, freedom of information and records management legislation.
Recommendations	The Council is asked to: 1. note the organisation's performance based on the statistical information provided.
Author	Caroline Gowans Information Governance Coordinator
Responsible Officer	Lynn Murray Interim Director of Finance and Resources Tel: 01382 721847
Link to Strategic Plan	The information in this report links to all of our strategic outcomes.
Link to the Risk Register	Risk 3: We fail to meet corporate governance, external scrutiny and legal obligations.
Equality Impact Assessment (EIA)	1. An EIA was not developed because this is a report about performance and therefore it does not propose a course of action that will have an impact on people with protected characteristics.
Documents attached	None
Background papers	None

1. EXECUTIVE SUMMARY

1.1 This report summarises key information governance statistics for the period 1 April 2020 to 31 March 2021. We identify any issues of concern that the Council needs to be aware of in relation to the organisation's compliance with data protection, freedom of information and records management legislation.

2. RECORDS MANAGEMENT

2.1 The Public Records (Scotland) Act 2011 requires Scottish public authorities to produce and submit a records management plan setting out proper arrangements for the management of public records for the Keeper of Records for Scotland to agree. The SSSC's records management plan was agreed in 2014 and we continue to meet the requirements of the legislation.

3. PERFORMANCE INFORMATION AND STATISTICS

Individual rights requests

3.1 The table below relates to individual rights requests, in particular those relating to the right of access (commonly referred to as a Subject Access Request (SAR)), the right to erasure (also known as the right to be forgotten) and the right to rectification. The organisation must respond to these types of requests normally within one calendar month.

Quarter	Total SARs received	Percentage responded to within statutory timescale	Total requests for rectification/erasure	Percentage responded to within statutory timescale
1	7	100%	0	N/A
2	9	100%	1	100%
3	12	100%	0	N/A
4	12	91.6%	1	100%

3.2 The statutory timescale was not met on one occasion during quarter four for a number of reasons. A higher volume of requests than is normal was received during a short period of time, placing unusually acute pressure on the Information Governance team. Other regulators have also experienced unusually high volumes during the pandemic. The late request was complex due to the nature and volume of information involved and the reduced outgoing mail service (due to the Covid pandemic) impacted on the

organisation's ability to respond to the request, in the format requested, on time. The requester was contacted to give them the option of receiving an email response to meet the deadline but they preferred to wait until it could be posted. We are now building into our timescales the reduced outgoing postal mail service.

Third Party Requests

3.3 Requests from regulatory bodies during the reporting period included Social Work England, Social Workers Registration Board New Zealand, Care Council Wales, CORU (Health and Social Care Council Ireland), Northern Ireland Social Care Council, General Pharmaceutical Council, NHS Education for Scotland, and the Office for Standards in Education.

3.4 Requests categorised as other include Lancashire Constabulary, City of London Police, a solicitor and First Advantage.

Quarter	Total Received	Regulatory Bodies	Police Scotland	Other
1	20	20	0	0
2	29	29	0	0
3	41	34	5	2
4	30	24	4	2

Data security incidents

3.5 The organisation is under a statutory duty to report certain personal data breaches to the Information Commissioners Office (ICO) within 72 hours of becoming aware of the breach, where feasible. The organisation has a data breach management process. This includes carrying out a risk assessment to determine whether a breach is reportable and an investigation to identify the cause and to recommend actions to prevent recurrence.

Quarter	Number of new incidents reported	Percentage risk assessed within 72 hours	Number of investigations completed
1	14	57.1%	14
2	19	78.9%	19
3	22	95.4%	22
4	29	96.5%	29

3.6 The percentage of incidents risk assessed within 72 hours improved considerably over the year. The failure to risk assess all incidents within 72 hours was due to a number of reasons, including: pressure on the Information Governance team's resources; the breach was not reported to the Information Governance team sufficiently early enough to allow the assessment to be completed on time. The Information Governance team has been and will continue to encourage early reporting of data security incidents across the departments within the organisation. We will carry out awareness raising of the reporting requirements and continue to carry out training as detailed at 3.15.

Data Security Reports to ICO

3.7 When a personal data breach has occurred, data controllers need to establish the likelihood and severity of the risk to people's rights and freedoms. If there is a significant risk we will notify the ICO.

Quarter	Numbers of reports to ICO	Number of cases where enforcement action was taken
1	0	N/A
2	1	0
3	0	N/A
4	0	N/A

3.8 The incident reported related to an unauthorised third-party access to a staff member's email account by hacking. No further action was taken by the ICO.

3.9 The following steps have been taken to ensure that the risk of a repeat of this incident is reduced.

- Multi-factor authentication has been implemented, requiring staff to add a second form of authentication at frequent intervals and where any device that has not previously accessed our systems tries to log in.

- Access has been blocked to D365 (the organisation's customer relationship management system) for any devices not located in the UK.

- A new IT security policy was created and published for staff. This policy includes a section on passwords.

- Digital Services are in the process of rolling out a new virtual private network (VPN), which will increase security arrangements by creating a VPN connection automatically when a member of staff connects to a non-work network. This will ensure that all traffic is filtered through an encrypted tunnel to our network and ensures our security policies and filtering rules apply.

Freedom of information (FoI) requests

3.10 The organisation must respond to FoI requests within 20 working days.

Quarter	Number of requests received	Percentage responded to within statutory timescale	Number of requests for a review received	Percentage of requests for review responded to within Statutory timescale
1	5	80%	1	100%
2	10	100%	0	N/A
3	11	100%	0	N/A
4	14	100%	1	N/A

3.11 The statutory timescale was not met on one occasion during quarter one. This was because the request was not forwarded to the Information Governance team in error. The information was provided to the applicant following receipt of a request for a review. We will issue reminders to staff to ensure that the risk of a repeat of this incident is reduced.

ICO/Scottish Information Commissioner (SIC) Appeals

3.12 Under the Freedom of Information (Scotland) Act 2002, an individual has the right of appeal to the SIC if they remain dissatisfied with our response following a request for a review.

3.13 Under data protection legislation, an individual has the right to make a complaint to the ICO if they remain dissatisfied with our handling of a rights request. There were no open cases with the ICO or SIC during the year and therefore no cases where enforcement action has been taken.

3.14 There were no appeals raised during this financial year.

Delivery of data protection training

3.15 The key performance indicator is that 100% of new starts are trained during their induction period.

3.16 44 members of staff joined the organisation during the reporting period. 86.4% of staff completed data protection training during their induction period. We have asked for the support of data champions to make sure that the remainder complete the training as soon as possible.

Delivery of records management training

3.17 Key performance indicator 1 is that 100% of staff receive refresher training within one year of completing the initial training.

3.18 Refresher training was issued to 100% of relevant staff during the reporting period. 88.9% of staff completed the training. Incomplete training was due to maternity leave, leavers, or long-term sickness absence.

3.19 Key performance indicator 2 is that 100% of new starts are trained during their induction period.

3.20 44 members of staff joined the organisation during the reporting period. 72.8% of staff completed records management training during their induction period. We are continuing to send out reminders to make sure the remainder complete the training as soon as possible. We will escalate to line managers where the training is not completed following reminders.

4. LEGAL IMPLICATIONS

4.1 The organisation is required to comply with certain obligations under the data protection, freedom of information and records management legislation. This report provides assurance that the organisation has sufficiently met those obligations during the previous financial year.

5. RESOURCE IMPLICATIONS

5.1 Despite the increase in the number of requests, the Information Governance team has achieved a high level of compliance with statutory timescales. Council has approved additional roles within the team to strengthen organisational compliance and reflect increased workloads.

6. STAKEHOLDER ENGAGEMENT

6.1 This is a governance report and therefore no stakeholder engagement was required.

7. IMPACT ON PEOPLE USING SOCIAL SERVICES AND CARERS

7.1 It is important that the SSSC is and is seen to be a well governed organisation. If the organisation does not meet its information governance obligations this would impact on the confidence of people who use services and their carers that the SSSC is effectively discharging its legal duties.

8. CONCLUSION

8.1 This report asks Council to note the organisation's compliance with its information governance obligations based on the statistical information provided. There are no significant concerns about the organisation's compliance.