Scottish Social Services Council

Council
25 August 2022
Agenda item: 17
Report no: 37/2022

Title of report	Annual Information Governance Report
Public/Confidential	Public
Summary/purpose of report	To provide 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	This report asks Council to endorse the organisation's performance in information governance compliance in the 2021/22 financial year.
Author	Caroline Gowans, Information Governance Coordinator
Responsible Officer	Lynn Murray, Interim Director, Finance and Resources
Link to Strategic Plan	The information in this report links to: Outcome 1: People who use services are protected by ensuring the regulated workforce is fit to practise. Outcome 2: The SSSC supports and enhances the development of the registered workforce to deliver high standards of practice and drive improvement. Outcome 3: Our workforce planning activities support employers, commissioners and policy makers to deliver a sustainable, integrated and innovative workforce. Outcome 4: The social work, social care and early years workforce is recognised as professional and regulated and valued for the difference it makes to people's lives.
Link to Risk Register	Risk 3: We fail to meet corporate governance, external scrutiny and legal obligations.
Impact assessments	1. An Equalities Impact Assessment (EIA) was not required.

	2. A Data Protection Impact Assessment (DPIA) was not required. 3. A Sustainability Impact Assessment (SIA) was not required.
Documents attached	None
Background papers	None

EXECUTIVE SUMMARY

1. This report summarises the performance of the SSSC in relation to information governance for the period 1 April 2021 to 31 March 2022. We identify any issues of concern that Council needs to be aware of in relation to the organisation’s compliance with data protection, freedom of information and records management legislation.

RECORDS MANAGEMENT

2. 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 (the Keeper) to agree. The Keeper agreed the SSSC’s records management plan in 2014.

3. The Keeper introduced a progress update review (PUR) mechanism, following the agreement of the SSSC’s records management plan in 2014. This mechanism allows us the opportunity to provide annual progress updates, concerning the records management plan, to the Keeper’s Assessment Team. The team’s assessment provides an informal indication of what marking we could expect when we submit a revised records management plan to the Keeper under the 2011 Act.

4. We submitted a PUR to the Keeper’s Assessment Team in January 2022 and they assessed our performance against our records management plan and produced a report on 22 March 2022. The Assessment Team concluded that we continue to properly consider the various elements in our plan and that we continue to meet the requirements of the legislation.

5. We are carrying out a long-term project to ensure the organisation continues to comply with its records management obligations, and completion of the planned areas of work will improve records management practices across the organisation. The areas of this project include:

   - resolution of SharePoint issues
   - review of our information asset register
   - comprehensive review of our retention schedule
   - preparation of SharePoint folder structures and files to implement auto-deletion policies
   - application of auto-delete policies
   - development and promotion of local naming conventions.

6. We provide records management training to all new starts during their induction period, and we provide refresher training to all staff annually. We have a high completion rate of over 90% for records management training.

DATA PROTECTION

Individual Rights Requests

7. Individual rights requests received in the reporting period include the right of access (commonly referred to as a Subject Access Request), 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 within one calendar month.

8. We responded to 91.1% of these requests within the statutory timescale in the reporting period. We do not have any concerns about our response rate. Late responses were isolated cases and were late for a variety of reasons, including a higher volume of requests than is normal during quarter 1, which placed acute pressure on the Information Governance team, repeated and complex requests, and we failed to meet the statutory timescale on one occasion due to an administrative error in forwarding the request to the Information Governance team.

9. We provide subject access statistics to the Audit and Assurance Committee through the assurance report on a quarterly basis.

10. Under data protection legislation, an individual has the right to make a complaint to the Information Commissioner's Office (ICO) if they remain dissatisfied with our handling of a rights request. There were no complaints raised with the ICO during the reporting period.

Third Party requests

11. We responded to 108 third party and other regulatory bodies requests during the reporting period. Requests from regulatory bodies were primarily from Social Work England. The number of requests remain consistent with financial year 2020/21, where we responded to 120 requests.

Data security incidents

12. The organisation is under a statutory duty to report certain personal data breaches to the 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 recurrences.

13. We received 85 data security incidents reports in the reporting period. We risk assessed 94.1% of these incidents within 72 hours. The failure to risk assess all incidents within 72 hours was due to pressure on the Information Governance team's resources or that the breach was not reported to the Information Governance team sufficiently early to allow them to complete the assessment on time.

14. The Information Governance team has and will continue to encourage early reporting of data security incidents across the departments within the organisation through awareness raising of the reporting requirements and training as detailed at paragraph 18.

15. As part of the risk assessment process, we categorise data security incidents as low/green, medium/amber, or high/red, dependant on factors such as the volume of data released, the sensitivity of the information released and the risk to the affected individuals. We report those categories classified as high/red to the ICO within 72 hours.

16. We reported one data security incident to the ICO in the reporting period. The incident concerned unauthorised disclosure of email addresses of participants of an online event to other participants. We took remedial action and the ICO took no further action.

17. We report incidents categorised as medium/amber and high/red to the Audit and Assurance Committee on a quarterly basis through the assurance report.

Delivery of data protection training

18. We appoint and train data champions for each team to provide bespoke training to all staff. We have a 100% completion rate for data protection training.

Data security procedures

19. We reviewed and updated the data security procedures for each team to include a new section on the data warehouse and visualisation tool and the approval process for future updates to the security procedures.

FREEDOM OF INFORMATION

20. The organisation must respond to freedom of information requests within 20 working days. We responded to 100% of the 32 requests in the reporting period, within the statutory timescale.

21. The number of requests remain consistent with financial year 2020/21, where we responded to 40 requests.

22. We provide freedom of information request statistics to the Audit and Assurance Committee through the assurance report on a quarterly basis.

23. Under the Freedom of Information (Scotland) Act 2002, an individual has the right of appeal to the Scottish Information Commissioner if they remain dissatisfied with our response following a request for a review. There were no appeals raised to the Scottish Information Commissioner during the reporting period.

Publication Scheme

24. We have reviewed and are updating our publication scheme to reflect information that we make routinely available to the public.

POLICIES

25. The Information Governance team reviewed and updated the following policies during the reporting period.

Records Management Policy

26. We reviewed the policy and made minor changes to reflect the new policy template and the organisational restructure since 2014. Council approved the policy in August 2021.

Data Protection Policy

27. We reviewed the policy and updated it to reflect the new policy template, references to legislation, extend our statement of intent, clarify our lawful basis for processing personal data, update the section on international transfers and include a section on roles and responsibilities. Council approved this policy in November 2021.

Secure Handling, Use, Storage, Retention and Destruction of Disclosure Information Policy

28. We reviewed and updated the policy to reflect the new policy template, and new legislation and processes that apply to the secure handing of disclosure information. The Executive Management Team (EMT) approved this policy in October 2021.

29. We are currently working with departments which handle disclosure information to make sure that we have operational procedures in place which cover the retention requirements set out in this policy.

CONSULTATION

30. We did not carry out any stakeholder engagement because this is a governance report about performance of the organisation. The Operational Management Team and EMT have endorsed the report.

RISKS

31. We have an averse risk appetite towards legal compliance. The ICO can impose sanctions for failure to meet data protection statutory obligations. There is also a risk of criminal or civil proceedings and reputational risk.

32. It is important that the SSSC is 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.

IMPLICATIONS

Resourcing

33. The SSSC has achieved a high level of compliance with statutory timescales.

34. Council approved an additional role within the team during this reporting period to strengthen organisational compliance and reflect increased workloads.

Compliance

35. The organisation must comply with our 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 this reporting period.

IMPACT ASSESSMENTS

Equalities

36. An Equalities Impact Assessment was not required 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.

CONCLUSION

37. This report asks Council to endorse the organisation's performance in information governance over the reporting period 1 April 2021 to 31 March 2022. There are no significant concerns about the organisation's compliance with the statutory requirements.