Council
25 May 2023
Agenda item: 09
Report no: 19/2023

Title of report	Information Governance Annual 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: 1. endorse the organisation's performance in information governance compliance in the 2022/23 financial year. 2. approve the amendments to the Data Protection Policy attached as Appendix 1 to this report.
Author	Caroline Gowans, Information Governance Coordinator
Responsible Officer	Hannah Coleman, Acting Director of Regulation
Link to Strategic Plan	The recommendations in this report link to: Outcome 1: **Trusted** People who use services are protected by a workforce that is fit to practise. Outcome 2: **Skilled** Our work supports the workforce to deliver high standards of professional practice. Outcome 3: **Confident** Our work enhances the confidence, competence and wellbeing of the workforce. Outcome 4: **Valued** The social work, social care and children and young people workforce is 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	Appendix 1: Data Protection Policy v2.1
Background papers	None

EXECUTIVE SUMMARY

1. This report summarises the performance of the SSSC in relation to information governance for the period 1 April 2022 to 31 March 2023. 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.

2. We have reviewed and updated our Data Protection Policy and present it to Council for approval.

RECORDS MANAGEMENT

3. 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.

4. 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.

5. We submitted a PUR to the Keeper's assessment team in January 2023 and we await the result.

6. 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 completed in the reporting period are:

    - resolution of SharePoint issues
    - review of our information asset register
    - comprehensive review of our retention schedule
    - development of bespoke local naming conventions for each department.

7. 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 completion rate of over 72% for records management training. We have asked for the support of line managers to manage their team's compliance, and we have issued reminders to all members of staff who have outstanding training.

DATA PROTECTION

Individual rights requests

8. 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), the right to rectification, and the right to object. The organisation must respond to these types of requests within one calendar month.

9. We received 43 requests and have a 100% response rate for compliance within the statutory timescales.

10. The number of requests remains consistent with financial year 2021/22, where we responded to 47 requests.

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

12. 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

13. We responded to 143 third party and other regulatory bodies requests during the reporting period. The number of requests has increased by 32.4% in comparison with financial year 2021/22, where we responded to 108 requests. We received a slight increase in the number of requests from Social Work England, Care Council for Wales, CORU and the Health and Care Professions Council in comparison to financial year 2021/22. In addition, we received an increased number of requests from other types of third-party organisations, for example international regulators and local authorities.

Data security incidents

14. 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.

15. We risk assessed 102 data security incidents reports in the reporting period. The number of data security incident reports increased by 20% in comparison with financial year 2021/22, where we received 85 reports. The increase is due to issues surrounding the role of countersignatories. A failure of third parties to report the termination of a countersignatory role was the reason for most of these incidents. We have introduced various mechanisms to combat this issue. We are also working with the

Communications team to issue regular reminders to employers and workers that they have an obligation to keep their records up to date, and to highlight the consequences of not updating countersignatory records.

16. 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 19.

17. 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.

18. We reported two data security incidents to the ICO in the reporting period. One incident concerned Fitness to Practise sending out hearing information to a registrant, which contained personal data, and one concerned Performance and Improvement sharing personal data of twenty-nine registrants with Public Health Scotland. We took remedial action and the ICO took no further action. Also, a member of the public submitted a complaint to the ICO in relation to an inappropriate disclosure of personal information about them to a registered worker, which we accepted. While the ICO concluded we did not comply with our data protection obligations they considered our full explanation of the circumstances alongside the steps we had taken in investigating and identifying the issues, implementing improvement measures, and apologising to the complainant were reasonable and decided to take no further regulatory action.

Delivery of data protection training

19. We appoint and train data champions for each team to provide bespoke training to all staff. We have an 92% completion rate for data protection training in the reporting period. We have asked for the support of data champions to make sure that the remainder complete the training as soon as possible.

Data security procedures

20. We regularly review and update the data security procedures where necessary following our security incident recommendations and the outcome of our bi-annual data trend report for the Operational Management Team. We also carry out an annual review in March each year.

21. We completed an ICO accountability self-assessment during the reporting period and are reviewing actions to take forward.

FREEDOM OF INFORMATION

22. The organisation must respond to freedom of information requests within 20 working days. We responded to 100% of the 33 requests in the reporting period, within the statutory timescales.

23. The number of requests remains consistent with financial year 2021/22, where we responded to 32 requests.

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

25. 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

26. This year, we reviewed and updated our publication scheme to reflect information that we make routinely available to the public. We also made improvements to the information provided on our website under the publication scheme.

POLICIES/PROCEDURES

27. The Information Governance team reviewed and updated the following policy and procedure during the reporting period.

Data Protection Policy

28. We reviewed the policy and updated to remove the requirement of an annual audit of our data security procedures. We are of the view that the annual audits are not effective as only a small number of staff are selected at random, and it is a time-consuming process. Instead, we have developed other more effective methods to embed good data protection practices within the organisation. We monitor compliance with the security procedures through security incident reports which we send to the relevant heads of department, and we follow up suggested remedial actions for red and amber categorised incidents. We also provide a data breach trend report to the Operational Management Team. These measures highlight if the security procedures are not being followed, and our recommendations will include that staff are reminded of their responsibility to follow these procedures. We will also schedule a yearly reminder to the Operational Management Team asking that they send a reminder to all staff in their respective departments. We are considering how Power BI can support our compliance work.

Retention Schedule

29. We reviewed and made substantial changes to our Retention and Disposal Schedule. We considered this necessary to reflect the structure of the

organisation and the additional information now held. Executive Management Team (EMT) approved the retention schedule on 21 December 2022.

30. The revised schedule will make sure that records retained by the SSSC are reliable, and we hold information no longer than necessary. This will make the process of locating records easier, and make sure that we are not wasting money or space (either digital or physical) by storing information that we do not require. It also makes sure that we are compliant with data protection legislation, which requires retention of information only for as long as necessary. Application of the new retention periods will also reduce workloads when we receive a request for information.

CONSULTATION

31. We did not carry out any stakeholder engagement because this is a governance report about performance of the organisation. EMT has endorsed the report and the amendments to the Data Protection Policy.

RISKS

32. 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. The Keeper of Records for Scotland has powers to undertake records management reviews and issue action notices for improvement, and the Scottish Information Commissioner has power to issue formal practice recommendations and enforcement notices.

33. 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

34. The SSSC has achieved a high level of compliance with statutory timescales. The recommendations in this report do not have any resourcing implications.

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 2022 to 31 March 2023. There are no concerns about the organisation's compliance with the statutory requirements.

38. This report also asks Council to approve the amendments to the Data Protection Policy.