**Council**
**23 May 2024**
**Agenda item: 08**
**Report no: 18/2024**

| | |
|---|---|
| **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** | The Council is asked to endorse<br>the organisation's performance in information governance compliance in the 2023/24 financial year. |
| **Author** | Anne Stewart, Head of Legal and Corporate Governance |
| **Responsible Officer** | Hannah Coleman, Acting Director, Regulation |
| **Link to Strategic Plan** | The information in this report links to:<br>Outcome 1: **Trusted** People who use services are protected by a workforce that is fit to practise.<br>Outcome 2: **Skilled** Our work supports the workforce to deliver high standards of professional practice.<br>Outcome 3: **Confident** Our work enhances the confidence, competence and wellbeing of the workforce.<br>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 Assessment** | An Impact Assessment (IA) 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 2023 to 31 March 2024. 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 continue to work on a long-term project to ensure the organisation complies with its records management obligations, and completion of the planned areas of work will improve records management practices across the organisation. Over the next few months, the SSSC Records Manager will progress a plan with support from colleagues across the organisation to review our records management structure and processes to ensure we have effective records management.

5. 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 85% for records management training. The figure for last year was 72%. We note that these figures do not take account of staff who are on long term sick or maternity leave. 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

6. 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.

7. We responded to 32 requests in the reporting period with 91% responded to within the statutory timescales. Last year we received 43 requests.

8. 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 was one complaint raised during the reporting period. The complaint concerned failure to confirm an address when responding to a Subject Access Request. The ICO investigated and we provided a full explanation of the circumstances alongside the steps we had taken to attempt to meet our statutory obligations. The ICO made a number of recommendations but took no further action. We have carried out a lessons learned with relevant staff members.

**Third Party requests**

9. We have changed our process on dealing with Third Party Requests. The Registration Team now deal with straightforward requests from Social Work England, Social Care Wales and the Northern Ireland Social Care Council. This means we no longer collate the number of requests within Legal and Corporate Governance (LCG). However, the LCG team deals with complex requests and requests from other types of third-party organisations, for example international regulators and local authorities.

**Data security incidents**

10. 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.

11. 83 data security incidents/breaches were reported over 2023/24, a reduction of 19% in comparison with financial year 2022/23, where we received 102 reports. We assessed these as nine near misses, 14 security incidents and 59 breaches. We categorise an incident as a breach where there was a failure in our security procedures. A security incident is one where information has been disclosed but there was no failure in our security procedures eg counter signatory details had not been updated by the employer.

12. 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 15.

13. 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.

14. We reported one data security incident to the ICO in the reporting period. The incident concerned disclosure of a data subject's street address within a Notice of Decision. We took remedial action and the ICO took no further action.

### Delivery of data protection training

15. We appoint and train data champions for each team to provide bespoke training to all staff. We have a completion rate of 80% for data protection training in the reporting period. Last year the figure was 92%. We note that these figures do not take account of staff who are on long term sick or maternity leave. We have asked for the support of data champions to make sure that the remainder complete the training as soon as possible and we are reviewing our processes to improve how we record and monitor completion of training.

### Data security procedures

16. We review and update the data security procedures where necessary following our security incident recommendations. We have also carried out an annual review.

17. We progressed our action plan which we put in place after completing the ICO accountability self-assessment. Actions completed in the reporting period include:

    a. Review of automated decision making
    b. Setting up of Information Governance Oversight Group which meets bi annually
    c. Setting up Data Champions quarterly meetings
    d. Promotion of Data Protection Policy to staff
    e. Review of privacy defaults on internet pages

## FREEDOM OF INFORMATION

### Requests for information

18. The organisation must respond to freedom of information requests within 20 working days.

19. We responded to 26 requests in the reporting period with 96% responded to within the statutory timescales. Last year we received 33 requests.

20. 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

21. We have made improvements to the information provided on our website under the publication scheme.

### Retention Schedule

22. We commenced a review of the Retention Schedule in 2023/24 and will submit this to EMT for approval shortly.

## CONSULTATION

23. We did not carry out any consultation in the preparation of this report.

## RISKS

24. We have an averse risk appetite towards governance matters. 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.

25. 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

26. There are no resource implications arising from recommendations in this report.

### Compliance

27. 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. There are no compliance implications arising from the recommendations in this report.

## IMPACT ASSESSMENT

28. An IA is not necessary as this report relates to internal governance matters.

## CONCLUSION

29. This report asks Council to endorse the organisation's performance in information governance over the reporting period 1 April 2023 to 31 March 2024. There are no concerns about the organisation's compliance with the statutory requirements.