Scottish Social Services Council

Council
25 May 2023
Agenda item: 09
Report no: 19/2023
Appendix 1

Data Protection Policy

May 2023

Document governance and management

Document owner/author/lead	Director of Regulation
Version number	2.1
Current version referred for approval to	
Date of next review	November 2024
Date of equality impact assessment (mandatory)	No EIA required. The change does not propose a course of action that will have an impact on people with protected characteristics.
Date of privacy impact assessment (if required)	N/A
Date of environmental impact assessment (if required)	N/A

Change log – for minor changes to spellings, sentences etc. Use when policy is not being put forward for approval.

Officer name	Date of change	Description of change	Confirm upload of revised document

Contents

1. Introduction

This is the Data Protection Policy adopted by the Scottish Social Services Council (SSSC).

For the purposes of data protection legislation, we are a data controller and a public authority.

The SSSC is committed to ensuring that we treat personal information lawfully and correctly. Data protection law contains certain safeguards which we must follow when we process personal data. This policy sets out how we intend to comply with data protection legislation and how we will handle personal data in a way which allows us to fulfil our statutory functions, uphold public confidence as an effective regulator and make sure we are a fair and effective employer.

'Personal data' is information which relates to an identifiable living individual, who can be directly or indirectly identified from the information.

We must collect and use personal data about individuals to fulfil our statutory functions under the Regulation of Care (Scotland) Act 2001 and other related functions. We collect and use personal data about:

- people who are applying to be registered or who are registered
- people who have not registered or applying to register but we have told them we process information about them
- people who use services
- employers and universities of social service workers and those who support them
- people who are applying for a postgraduate student bursary and their parents/spouse/civil partner/co-habitee
- Fitness to Practise hearing witnesses
- people who have complained about someone who may be a social service worker
- people who have complained about the SSSC
- prospective employees and Panel Member applicants
- current and former employees and current and former Panel Members
- Council Members
- people or organisations that we procure goods and services from people or organisations that we contract with
- event attendees
- people who make general or information governance enquiries
- employees of higher education institutions delivering approved courses
- people who have completed an Expression of Interest Form for the Health & Social Care COVID-19 Accelerated Recruitment portal website
- others we might communicate with.

We may be legally required to collect and use personal data to comply with the requirements of other public bodies, government departments or legislation.

2. Statement of intent

We process all personal data in compliance with the principles and safeguards set out in the data protection legislation. The data protection legislation includes:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (the Act)
- The Privacy and Electronic Communications Regulations 2003.

Anyone who processes personal data on behalf of the SSSC must comply with this policy and the data protection legislation.

The SSSC is committed to adopting a culture of 'data protection by design and default'. This includes:

- considering data protection issues and risks as part of the design and implementation of systems, services, and business practices
- making sure we have adequate technical and organisational measures in place to ensure the security of data
- making sure that our systems and technologies are capable of adequately protecting personal data
- having robust security incident reporting and management processes in place
- embedding data protection impact assessments (DPIAs) into relevant processes where appropriate (or required)
- documenting data sharing and making sure we have agreements in place, when required.

The SSSC is committed to upholding the rights of individuals in relation to their personal data and will comply with individuals' requests in relation to their personal data where legally required to do so (see section 9 below).

Data protection training is a fundamental aspect of our data protection compliance. Staff must receive training, appropriate to their role, to help them understand how to process personal data in line with this policy (and other associated policies, procedures, and guidance). Data protection guidance is also available to staff on the intranet.

3. Aims

This policy aims to:

- state our commitment to compliance with data protection legislation and the principles of the data protection legislation

- set out how we will comply with the data protection legislation using technical and organisational measures, and in particular, the principles of data protection by design and default
- demonstrate that we have relevant data protection policies in place as required by the data protection legislation
- provide a general appropriate policy document and an overarching appropriate policy document for processing of special categories of personal data
- state the responsibility of everyone working for and on our behalf so that we comply with the principles of the data protection legislation
- set out some of the circumstances that we are exempt from certain general principles in exercising our statutory functions as a regulator.

4. Roles and responsibilities

4.1 Council

The Council is accountable for:

- approving this policy
- making sure this policy complies with data protection legislation and does not breach any other statutory requirement placed upon the SSSC
- making sure the structure of the organisation is fit for purpose to deliver our objectives
- making sure the Chief Executive, Executive Management Team (which includes the Senior Information Risk Owner) and the Data Protection Officer have in place appropriate and up to date policies and procedures to comply with data protection legislation.

4.2 Executive Management Team

The Executive Management Team is responsible for:

- making sure that all collection and processing of personal data within their respective areas of responsibility complies with this policy
- making sure that personal data processed by third parties within their respective areas of responsibility complies with this policy
- approving Data Sharing Agreements within their respective areas of responsibility, in consultation with the DPO.

4.3 Senior Information Risk Owner

The Director of Regulation ~~Finance and Resources~~ is the SSSC's Senior Information Risk Owner (SIRO). The SIRO has strategic responsibility for governance in relation to data protection risks, with specific responsibility for:

- making sure the SSSC has the appropriate polices and processes in place to comply with data protection legislation
- overseeing the reporting and management of information incidents
- providing assurance to the Executive Management Team that information governance standards and performance are maintained
- appointing and line managing the SSSC's Data Protection Officer (DPO) who provides advice and assurances to the SIRO and carries out the duties of a DPO as detailed at 4.4

4.4 Data Protection Officer (DPO)

The SSSC's DPO is the Head of Legal and Corporate Governance.

The role of the DPO is to:

- inform and advise Council and staff about their obligations to comply with the UK General Data Protection Regulation (UK GDPR) and other data protection laws
- monitor compliance with the UK GDPR and other data protection laws, including the assignment of responsibilities, awareness raising, and training of staff involved in the processing operations ~~and related audits~~
- make sure that we implement and keep up to date the Data Protection Policy and related procedures, controls, guidance, and templates
- provide advice on data protection impact assessments
- provide guidance and advice on specific data protection issues and compliance requirements
- act as the contact point for the Information Commissioner's Office on issues related to the processing of personal data.

The DPO also has the responsibilities set out in the data protection legislation for the role.

4.5 Information Governance Team

The Information Governance Team will support the DPO in maintaining compliance with the data protection legislation through development and implementation of this policy and related procedures, controls, guidance, and templates.
The Information Governance Team deal with requests to exercise data subjects' individual rights in terms of data protection legislation, in consultation with the Head of Department, where appropriate.

4.6 Operational Management Team

The Operational Management Team is responsible for:

- making sure that their staff are aware of this policy and related procedures, controls, guidance, and templates.
- implementing and ensuring compliance with data security procedures within their respective areas, taking advice from the DPO where required. This includes the requirement to take all reasonable steps to ensure compliance by third parties. ~~This also includes approving the annual audit of departmental data security procedures, in consultation with the DPO.~~
- assisting with the maintenance and revision of the retention and disposal schedule at operational level
- assisting with development, maintenance, and revision of the Information Asset Register
- ensuring implementation of relevant actions and recommendations identified through the security incident risk assessment process
- approving data protection impact assessments for their respective area, in consultation with the DPO
- designating appropriate staff members as Data Champions.

4.7 Data Champions

The role of a data champion is to:

- assist the development of bespoke data protection training for their departments
- provide general advice and assistance to the departments about their obligations under the data protection legislation
- seek advice from or escalate matters to the Information Governance Team where necessary
- ~~work with the Information Governance Team to complete the annual audits of security procedures which will be approved by OMT, in consultation with the DPO~~.

The Information Governance Team provides training to the Data Champions.

4.8 Line Managers

Line managers are responsible for making sure that their staff complete training for their role, to help them understand how to process personal data in line with this policy.

4.9 Staff

All SSSC staff must comply with this policy (and associated policies and procedures) when carrying out data processing activities. Specifically, staff must make sure that:

- they have sufficient knowledge and understanding of data protection, and that they undertake appropriate training on this subject as and when required to do so
- they process personal data only as necessary in the course of their duties or job role
- they seek advice from their Data Champion, manager or from the Information Governance Team where there is uncertainty about the appropriate action to take when processing personal data
- they can recognise a potential or actual security incident, and understand the internal reporting requirements relating to such an incident
- they can recognise a request from a data subject to exercise their rights under data protection legislation and can deal with any such request in a timely manner
- they cooperate with any actions required to mitigate or investigate a security incident, or to fulfil a request by a data subject to exercise their rights.

There may be other situations relating to the processing or use of personal data that are not on the above list. Members of staff should contact the Information Governance Team if they have any queries about the use or processing of personal data.

Staff must always contact the Information Governance Team if they:

- are unsure about what security or other measures they need to implement to protect personal data
- are unsure of the lawful basis that they are relying on to process personal data
- need to rely on consent for processing personal data
- need to prepare or update a privacy notice or other transparency information

- are unsure about the retention period
- are carrying out any activity that is likely to need a data protection impact assessment
- plan to use personal data for a different purpose than that for which it was originally collected
- plan to carry out activities involving automated processing such as profiling or decision making
- are entering into a contract with a third party that involves the processing or sharing of personal data.

5. Data protection principles

Article 5 of the GDPR sets out six data protection principles and we will comply with these principles when we process personal data. The principles are that data will be:

- processed lawfully, fairly and in a transparent way in relation to individuals ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes ('purpose limitation')
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation')
- accurate and, where necessary, kept up to date ('accuracy')
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed ('storage limitation')
- processed securely, including using appropriate technical or organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage ('integrity and confidentiality').

In accordance with Article 5(2), SSSC (as data controller) is responsible for demonstrating, and must be able to demonstrate, compliance with the above principles ('accountability').

6. Processing and use of personal data

We maintain a general record of processing which sets out how we process data in accordance with data protection legislation.

We mostly collect data about those listed under section one of this policy.

- All personal data processing must have a lawful basis for processing. Article 6(1) of the GDPR provides the lawful bases for the processing of personal data.

Our processing activities are carried out under the lawful basis set out in Article 6(e) of the GDPR unless stated otherwise. This means we process data "to perform a specific task in the public interest that is set out in law or in the exercise of official authority vested in the controller". This is because most of the processing of personal data that we do relates to carrying out our functions under the Regulation of Care (Sc) Act 2010.

Sometimes, we may rely on the consent of the data subject eg communications with the data subject for marketing, surveys or information purposes.

Our privacy notice details where the lawful basis is not a public task.

7. Special category data and data relating to criminal offences or convictions

We process certain special category personal data in connection with our role as an employer and to fulfil our statutory functions as a regulator. For example, we may:

- process personal data that reveals the racial or ethnic origin of an individual
- investigate allegations relating to the health of an individual
- process data relating to criminal offences or convictions.

In most cases, the lawful bases for processing these types of special category data are that it is necessary:

- for us to carry out the obligations and specific rights as an employer
- for us to pursue or defend any legal claims or court actions
- to fulfil our statutory functions and is in the substantial public interest
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided we put in place suitable safeguards to protect the fundamental rights and freedoms of the data subject
- to promote or maintain the equality of opportunity or treatment between groups of people
- for the prevention or detection of an unlawful act and we must carry it out without the consent of the data subject to prevent prejudice to those purposes and is necessary for reasons of substantial public interest

- to protect the public against dishonesty, malpractice, serious improper conduct, unfitness, incompetence or mismanagement in administration and we must carry it out without the consent of the data subject and is necessary for reasons of substantial public interest

- to comply with or assist others to comply with a regulatory requirement to decide if someone has committed an unlawful act or been involved in dishonesty, malpractice or seriously improper conduct, we cannot reasonably obtain consent and it is necessary for reasons of substantial public interest.

We will record the legal basis for any data processed which does not fall within any of the above.

8. Implementation

This section aims to set out how we process data in accordance with the data protection principles.

Lawfulness, fairness and transparency

We:

- identify an appropriate lawful basis (or bases) for processing personal data, including if special category personal data or when processing criminal offence data

- will not do anything unlawful with personal data

- consider how the processing of personal data may affect the people concerned and will justify any adverse impact

- only handle people's data in ways they would reasonably expect, or be able to explain why any unexpected processing is justified

- do not deceive or mislead people when we collect their personal data

- are open and honest and comply with the transparency obligations of the right to be informed.

As a regulator, we are exempt from certain obligations to provide fair processing information and other data subject rights if the exercise of those rights would prejudice the work we do. We may not make information available if we process personal data to give legal advice, for the purpose of legal proceedings and prospective legal proceedings or to share information with the police or other relevant bodies.

Purpose limitation

We:

- clearly identify and document our purpose or purposes for processing data

- include details of our purposes in our privacy information for individuals
- regularly review our processing and, where necessary, update documentation and privacy information for individuals
- make sure that any plans to use personal data for a new purpose is compatible with the original purpose and, if not, get consent or have a clear lawful basis for the new purpose.

Data minimisation

We:

- only collect personal data needed for our specified purposes
- have sufficient personal data to properly fulfill those purposes
- periodically review the data we hold and delete anything no longer needed
- handle personal data through appropriate corporate systems only
- monitor the use of data to make sure staff and contractors only process personal data to carry out their role.

Accuracy

We:

- ensure, where possible, the accuracy of any personal data we create
- have appropriate processes in place to check, where possible, the accuracy of the data we hold and record the source of that data
- have a process in place to identify when we need to keep the data updated to properly fulfill our purpose, and update it as necessary
- keep a record of any mistakes and make these clearly identifiable
- comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data
- as a matter of good practice, keep a note of any challenges to the accuracy of the personal data.

In some circumstances we may need to hold factually inaccurate information or an opinion that someone disagrees with as part of our statutory functions.

Storage limitation

We:

- know what personal data we hold and why it's needed
- carefully consider and can justify how long we keep personal data for
- have a policy with standard retention periods where possible, in line with our statutory functions

- regularly review our information and erase or anonymise personal data when it's no longer needed
- have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'
- clearly identify any personal data we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

As a regulator, we may need to keep some personal data for long periods of time. For example, fitness to practise case files are kept for a significant period after the case has concluded. We do this as we may need to refer to the earlier file if a new issue is raised about a worker or we're challenged about our decision making.

Information about our retention periods is available in our ~~retention policy~~ retention schedule.

Integrity and confidentiality (security)

We:

- have appropriate security measures in place to protect the personal data we hold
- develop, implement, and maintain appropriate data security systems to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed
- regularly review, evaluate, and test the effectiveness of our data security systems.

Accountability

We:

- take responsibility for what we do with personal data and how we comply with the other principles
- have appropriate measures and records in place to demonstrate compliance, such as:
    - adopting and implementing data protection policies, where appropriate
    - taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations
    - putting written contracts in place with organisations that process personal data on our behalf
    - maintaining documentation of our processing activities
    - implementing appropriate security measures
    - recording and, where necessary, reporting personal data security incidents

- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests
- appointing a data protection officer
- adhering to relevant codes of conduct and signing up to certification schemes, where possible

- review and update our accountability measures at appropriate intervals.

9. Individual rights

We make sure that people that we hold information on can fully exercise their rights under the Act, subject to exemptions under the data protection legislation. These include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights in relation to automated decision making and profiling.

10. Personal data security incidents

We make sure all staff can recognise a potential or actual security incident and immediately report any loss or suspected loss of personal data to their manager, head of department and to the Head of Legal and Corporate Governance, who is also the DPO. We may take disciplinary action for failure to report any such loss or suspected loss.

11. International transfers

We make sure we only transfer personal data outside of the United Kingdom in compliance with the conditions for transfer set out in chapter five of the GDPR.

12. Monitoring

We make sure:

- there is an individual with specific responsibility for data protection in the organisation
- all staff managing and handling personal information understand that they are responsible for following good data protection practice
- we train all staff managing and handling personal information

- we appropriately supervise all staff managing and handling personal information
- individuals who wish to make enquiries about handling personal information know who to contact and that we deal with such queries promptly, fairly, and courteously
- we clearly describe methods of handling personal information
- ~~we carry out an annual review and audit of our processing~~
- we regularly assess and evaluate performance in handling personal data.

13. Data Protection Impact Assessments

We consider the need for and, if necessary, carry out data protection impact assessments (DPIAs). We always consult the DPO when completing a DPIA and keep an appropriate record.

We carry out a DPIA:

- when a new processing activity is likely to result in a high risk to the rights and freedoms of the data subject
- for major system programmes, or a review of such programmes which involve:
  - the use of new or changing technologies
  - the systematic and extensive profiling or automated decision making to make significant decisions about people
  - large scale processing of special category or other sensitive personal data
  - the monitoring of a publicly accessible place on a large scale
  - the use of profiling, automated decision making or special category data to help make decisions on someone's access to a service, opportunity or benefit
  - profiling on a large scale.

We may carry out a DPIA from time to time even if it is not necessary to do so. We are mindful of our obligations under the data protection legislation when deciding whether to carry out a DPIA.

If a DPIA is completed, we will store a record with the DPO.

DPIA guidance is available for staff on the intranet.

Automated processing and decision making

We tell the data subject the reasons for the decision making or profiling and any consequences of this. We give the data subject the right to request human intervention or to challenge the decision.

Data processors

We may instruct other organisations to process personal data on our behalf. In such cases, we carry out checks to make sure the data processor has appropriate technical and organisational measures in place to meet the requirements of the data protection legislation. The Legal and Corporate Governance department can advise on contractual arrangements with data processors.

Data sharing

We make sure sharing of data with third parties complies with relevant data protection policies and Information Commissioner's Office guidance such as the Data Sharing Code of Practice.

Complaints procedure

Anyone who feels that we have not followed this policy can make a complaint through our complaints procedure and we will report the complaint to the Data Protection Officer who will advise on the response.

Scottish Social Services Council
Compass House
11 Riverside Drive
Dundee
DD1 4NY

Tel: 0345 60 30 891
Email: enquiries@sssc.uk.com
Web: www.sssc.uk.com

If you would like this document in a different format, for example, in larger print or audio-format, or in another language please contact the SSSC on 0345 60 30 891.
We promote equality by removing unlawful and unfair treatment on the grounds of any protected characteristic wherever possible.