Scottish Social Services Council

Council
21 November 2024
Agenda item: 13
Appendix 1

Data Protection Policy

November 2024

Introduction

The SSSC is committed to ensuring that we treat Personal data 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 guidance issued by the Information Commissioner's Office (ICO) 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.

This policy:

- states our commitment to compliance with Data protection legislation and the underlying principles
- sets 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
- demonstrates that we have relevant data protection policies in place as required by the Data protection legislation
- provides a general appropriate policy document and an overarching appropriate policy document for processing of special category Personal data and criminal offence data
- states the responsibility of everyone working for and on our behalf to comply with the principles of the Data protection legislation
- sets out some of the circumstances that we are exempt from certain general principles in exercising our statutory functions as a regulator.

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. This includes special category data and criminal data as detailed in section 1.2.

This policy applies to all processing of Personal data carried out by the SSSC.

It applies to temporary and permanent SSSC workers (employees, agency staff, contractors and student placements), Council and Panel Members and anyone else carrying out processing of Personal data on our behalf.

Contents

1. Policy

1.1 Data protection principles

The SSSC complies with Data protection legislation guided by the six 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 and record this
- 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
- are open and honest and comply with the transparency obligations of the right to be informed
- provide information on processing of Personal data in our privacy notice and other communications.

Purpose limitation

We:

- identify and document our purpose or purposes for processing data
- include details of our purposes in our privacy notice
- regularly review our processing and, where necessary, update documentation and privacy notice
- make sure that any plans to use Personal data for a new purpose is compatible with the original purpose and, if not, have a lawful basis for the new purpose and we tell the Data subject.

Data minimisation

We:

- only collect personal data that is adequate, relevant and limited to what is necessary for our purposes
- have sufficient Personal data to fulfill those purposes
- regularly review the data we hold and delete anything no longer needed
- monitor the use of data to make sure SSSC workers, Council Members and Panel Members and anyone else only process Personal data to carry out their role or for SSSC purposes.

Accuracy

We:

- ensure, where possible, the accuracy of any Personal data we create
- have processes in place to check, where possible, the accuracy of the Personal data we hold and record the source of that data
- have a process in place to identify when we need to keep the Personal 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 is no longer needed
- have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'

- 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 are challenged about our decision making.

Information about our retention periods is available in our retention and disposal schedule.

Integrity and confidentiality (security)

We:

- 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
- have robust processes in place to manage data security incidents

Accountability

We:

- 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.

We maintain a general record of processing which sets out how we process data in accordance with data protection laws. This is our Information Asset Register.

The accountability principle requires the SSSC (as Data controller) to demonstrate our compliance with the above principles and make sure we do not put individuals at risk because of processing their Personal data. The SSSC is committed to the accountability principle and regularly reviews its processes and procedures against the Information Commissioner's Office self assessment model.

1.2 Special category data and Criminal offence data

We process certain special category Personal data and criminal offence data in connection with our role as an employer and to fulfil our statutory functions as a regulator.

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

- for us to carry out our obligations and rights as an employer eg processing staff sickness absences, carrying out pre employment checks
- to fulfil our statutory functions and is in the substantial public interest eg as part of the Fitness to Practice investigations we process allegations relating to the health of a registrant or data relating to criminal offences or convictions
- 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, unfitness or incompetence 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, unfitness or incompetence, we cannot reasonably obtain consent and it is necessary for reasons of substantial public interest.

1.3 Individual rights

We make sure that people can exercise their information rights. 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 the rights in relation to automated decision making and profiling.

1.4 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 Information Governance Team. We may take disciplinary action for failure to report any such loss or suspected loss.

1.5 Data Protection by Design and Default

We have processes in place to ensure compliance and privacy by design is integral to processing of Personal data and carry out data protection impact assessments (DPIAs) when necessary. The DPO and Information Asset Owner sign off the DPIAs.

DPIA guidance is available for staff on the intranet.

We may complete a data processing checklist for processing where this is no or minimal risk to the Data subject.

1.6 Automated processing and decision making

Our privacy notice tells people about our automated processing and decision making.

1.7 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.

1.8 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.

We keep a register of our data sharing agreements.

1.9 International transfers

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

1.10 Monitoring

We make sure we:

- carry out regular reviews of our processing
- regularly assess and evaluate performance in handling Personal data
- regularly report on our compliance with Data protection legislation.

2. Roles and responsibilities

2.1 Council

Responsible for:

- approving this policy
- making sure the Chief Executive, EMT (which includes the SIRO) and the DPO have in place appropriate and up to date policies and procedures to comply with Data protection legislation.

2.2 Executive Management Team (EMT)

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.

2.3 Senior Information Risk Owner (SIRO)

The Director of Regulation is the SSSC's SIRO. The SIRO has strategic responsibility for governance in relation to data protection risks and responsible 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 security incidents
- providing assurance to the EMT that information governance standards and performance are maintained
- appointing and line managing the SSSC's DPO who provides advice and assurances to the SIRO and carries out the duties of a DPO as detailed at 2.4.

2.4 Data Protection Officer (DPO)

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

Responsible for:

- informing and advising about our obligations to comply with Data protection legislation
- monitoring compliance with Data protection legislation including the assignment of responsibilities, awareness raising, and training of staff
- making sure that we implement and keep up to date this policy and related procedures, controls, guidance, and templates
- providing advice and sign off data protection impact assessments
- providing guidance and advice on specific data protection issues and compliance requirements
- acting as the contact 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.

2.5 Information Governance Team (IGT)

The IGT 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 IGT deal with requests to exercise data subjects' individual rights in terms of Data protection legislation, in consultation with the head of department, where

appropriate.

The IGT trains and supports the Data Champions.

2.6 Operational Management Team (OMT) & Information Governance Oversight Group

The Information Governance Oversight Group is made up of the OMT and is responsible for:

- considering data protection topics
- supporting and complementing the DPO role
- working with the DPO in escalating significant issues and risks to EMT and Council
- supporting their Data Champions

The OMT are also Information Asset Owners and 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 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 for their information assets
- 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.

2.7 Data Champions

Responsible for:

- developing and delivering bespoke data protection training for their departments
- providing general advice and assistance to the departments about their obligations under Data protection legislation

- seeking advice from or escalating matters to the IGT where necessary

The IGT provides training to the Data Champions.

The Data Champions meet quarterly with the IGT to discuss issues and concerns.

2.8 Line Managers

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.

2.9 All who process Personal data on our behalf

Anyone who processes Personal data must comply with this policy (and associated policies and procedures) when carrying out SSSC data processing activities. Specifically, they 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 IGT 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 UK GDPR 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.

3. Further Information

3.1 Learning and Development

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, from Data Champions and the IGT.

3.2 Data protection procedures and documents

Links to the following data protection procedures and documents are found here.

Data processing checklist
Data Protection Impact Assessment
Information Asset Register
Privacy Notice
Records Management Policy
Retention and Disposal Schedule
Departmental security procedures

4. Document governance and management

Document owner/author/lead	Acting Director of Regulation
Version number	3.0
Current version referred for approval to	Council
Date of next review	November 2027
Date of impact assessment (if required)	November 2024

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

Appendix

Glossary

Criminal offence data – personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

Data controller – a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data.

Data processor – any person (other than data controller employee) who processes data on behalf of a data controller.

Data protection legislation – UK General Data Protection Regulation 2016/679 (UK GDPR), Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 which together govern the processing of personal data.

Data subject – any living individual who is the subject of personal data.

Information Asset Owner – the individual who has information management responsibilities for each SSSC information asset

Information Asset Register – a general record of processing which sets how we process personal data in line with data protection legislation.

Personal data – information which relates to an identifiable living individual, who can be directly or indirectly identified from the information. This includes identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It also includes any expression of opinion about the individual and indication of intention towards the individual.

Processing – any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special category personal data – personal data which is more sensitive and afforded more protection. This is information related to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person’s sex life or sexual orientation.

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.