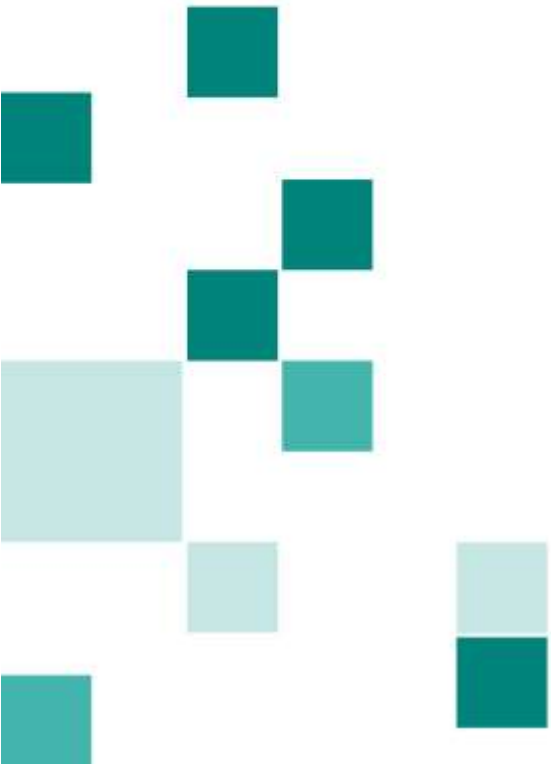
Scottish Social Services Council

Data Protection Policy

October 2018



Contents

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.

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 the public confidence as an effective regulator and make sure we are a fair and effective employer.

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 are working in social care but not registered
- people who use services
- employers and universities of social service workers and those who support them
- Fitness to Practise hearing witnesses
- people who have complained about someone who may be a social service worker
- 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
- 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.

Statement of intent

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

- The General Data Protection Regulation (GDPR)
- The applied GDPR
- The Data Protection Act 2018 (the Act)
- Regulations made under the Act and
- Regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive.

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 through the use of technical and organisational measures and in particular the principles of data protection by design and default
- demonstrate that relevant data protection policies are 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.

Roles and responsibilities

The Chief Executive and Council are ultimately responsible for the our compliance with data protection legislation. The Executive Management Team is responsible for approving this policy.

The Data Protection Officer has the responsibilities set out in the data protection legislation as well as maintaining this policy.

Managers in every department are responsible for implementing and ensuring compliance with data protection procedures. This includes the requirement to take all reasonable steps to ensure compliance with third parties.

We will designate appropriate staff members as Data Champions in each department. They will:

- be trained in the relevant provisions of the data protection legislation
- 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.

Managers and/or Data Champions 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 what the lawful basis that they are relying on to process personal data is
- 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.

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.

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 they are 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 are 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').

Article 5(2) states that the data controller is responsible for demonstrating, and should be able to demonstrate, compliance with the above principles ('accountability').

Processing and use of personal data

We will 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.

Article 6(1) of the GDPR provides the lawful basis for the processing of personal data. When processing data, we rely on the lawful basis that the processing is necessary for. These might be that the processing is necessary for:

- the performance of a contract with the data subject or when entering into a contract with the data subject
- compliance with a legal obligation
- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

In some cases we will also rely on the consent of the data subject. This is rare and tends to relate to communications with the data subject for marketing or information purposes.

We will record the legal basis that we process data for when it does not fall within any of the above principles.

Special category data

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
- for fulfilling 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 suitable safeguards are put in place 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 must be carried 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 must be carried out without the consent of the data subject and is necessary for reasons of substantial public interest
- for complying with or assisting 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.

Implementation

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

Lawfulness, fairness and transparency

We will:

- identify an appropriate lawful basis (or bases) for when processing personal data, including if special category personal data or criminal offence data is being processed
- not do anything generally unlawful with personal data
- consider how the processing of personal data may affect the people concerned and will justify any adverse impact
- only handle peoples data in ways they would reasonably expect, or be able to explain why any unexpected processing is justified
- not deceive or mislead people when their personal data is collected
- be 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 processing 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 will:

- clearly identify and document our purpose or purposes reasons 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 will:

- 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 will:

- 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 will:

- know what personal data we hold and why it's needed
- carefully consider and be able to 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 of time after the case has concluded. We do this as we may need to refer back 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 are available in our retention policy.

Integrity and confidentiality (security)

We will:

- 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 will:

- 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 be able 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 breaches
    - 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.

Individual rights

We will make sure the rights of people about whom information is held can be fully exercised 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.

Where an exemption exists, we will make sure there is a clear lawful basis for applying it.

Personal data breaches

We will make sure all staff 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 Data Protection Officer. Failure to report any such loss or suspected loss may constitute a disciplinary offence.

International transfers

We will make sure we only transfer personal data outside of the European Economic Area (EEA) in compliance with the conditions for transfer set out in chapter five of the GDPR.

Monitoring

We will 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
- all staff managing and handling personal information are appropriately trained to do so
- all staff managing and handling personal information are appropriately supervised

- individuals who wish to make enquiries about handling personal information know who to contact and that such queries are promptly, fairly and courteously dealt with
- methods of handling personal information are clearly described
- an annual review and audit is made of the way personal data is managed
- methods of handling personal data are regularly assessed and evaluated
- we regularly assess and evaluate performance in handling personal data.

Data Protection Impact Assessments

We will consider the need for and, if necessary, carry out Data Protection Impact Assessments (DPIAs). We will consult the Data Protection Officer at all times when completing a DPIA and keep an appropriate record.

We will 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. At all times, we will be mindful of our obligations under the data protection legislation when deciding whether or not to carry out a DPIA.

If a DPIA is completed, a record will be stored with the Data Protection Officer.

Automated processing and decision making

Generally, we will not engage in automated processing, profiling or automated decision making. Rule based logic supports some of our functions for the benefit and convenience of our stakeholders.

If we do use automated decision making or profiling, we will tell the data subject the reasons for the decision making or profiling and any consequences of this. We

will 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 will carry out due diligence 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 may be asked to advise on contractual arrangements with data processors.

Data sharing

We will ensure that any sharing of data with third parties complies with relevant data protection policies.

Complaints procedure

Anyone who feels that we have not followed this policy may make a complaint through our complaints procedure and we will report the complaint to the Data Protection Officer who may 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 another format, please contact the SSSC on 0345 60 30 891