Information Governance

Data Protection Policy

For: ALL STAFF and DATA SUBJECTS	Version 1.0 May 2018	Author: Ava Wieclawska

Key points:

- **This Data Protection Policy has been produced to set out SCRA's responsibilities in relation to data protection law; to outline the key principles; to clarify roles and responsibilities; and to identify appropriate procedures and guidance to help support compliance.**
- **It is the responsibility of all staff to familiarise themselves with this policy and its associated guidance and procedures.**
- **Internal and external data protection queries should be directed to SCRA's Information Governance Officer (Data Protection Officer) at Inforequest@scra.gsi.gov.uk or ava.wieclawska@scra.gsi.gov.uk, 0131 244 9157.**

1. Scope and purpose of this policy

1.1 SCRA is a data controller for all personal data[1] it processes in relation to its statutory functions within the Children's Hearings System. This includes the personal data of children, young people and their families, witnesses, associates, and victims of youth offending. SCRA processes the personal data of panel members and other professionals working within the Children's Hearings System in the delivery of its statutory functions and as an employer, SCRA processes the personal data of its staff and Board members, including secondments, contractors and temporary employees. Further details of the types of personal data[2] processed by SCRA, as well as the lawful basis for processing, can be found in SCRA's Record of Processing Activities.

1.2 SCRA is committed to protecting the rights and privacy of individuals in accordance with the requirements of data protection law and this policy has been produced to outline that commitment.

[1] Information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. For example, name, identification number, location data or online identifier. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of personal data depending on how difficult it is to attribute the pseudonym to a particular individual.

[2] Including Special Category Data and data relating to criminal convictions.

1.3 All SCRA staff should read and understand this policy and adhere to it in practice. Data subjects are advised to read this policy for information on the policies and procedures in place to protect their personal data.

1.4 This policy applies to all personal data for which SCRA is responsible, regardless of the format (paper or electronic data, including emails, photographs, video, CCTV and sound recordings).

2. Principles

2.1 In order to comply with data protection law, personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

This means that SCRA must:

- ensure there is a legal basis for processing personal data;
- inform individuals about our lawful basis for processing their personal data;
- be transparent about our data processing activities; and
- tell individuals what we will do with their personal data and what rights they have in respect of the data processing.

Staff must not knowingly do anything unlawful with personal information, or allow others to do so, including using it for purposes the individual is unaware of and would not reasonably expect.

We will comply with this principle by:

- identifying our legal basis for processing in our privacy notices and Record of Processing Activities supporting documentation;
- explaining who we are, what personal data we process and how it will be processed (including details of who has access to the data and who it will be shared with) in our privacy notices; and
- establishing Data Processing Contracts and Information Sharing Protocols with key partners and data processors to identify the lawful basis for sharing data and clearly identify roles and responsibilities of each party in respect of the personal data being shared or processed.

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

This means that SCRA must:

- ensure that personal data is collected for specific purposes; and
- that the data is not further processed for purposes that are considered incompatible with the original purposes.

We will comply with this principle by:

- ensuring that all staff in SCRA are aware of the legal basis and purposes for processing personal data and that they must not further process personal data for incompatible purposes; and
- telling individuals about any new uses of their personal data (and the relevant lawful basis) before starting the processing.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

This means that SCRA must:

- ensure that we only hold personal data that is adequate for the purposes for processing;
- not process more information about an individual than we need for that purpose; and
- not process excessive amounts of data.

We will comply with this principle by:

- challenging partner agencies when we consider excessive data to have been shared with SCRA, that are out with our purposes for processing;
- utilising measures of data minimisation where appropriate so that we only collect and process the data that we need to fulfill the relevant purposes; and
- retaining evidence of discussions with partner agencies when we consider excessive data to have been shared.

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

This means that SCRA must:

- take reasonable steps to ensure the accuracy of any personal data we process;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

We will comply with this principle by:

- accurately recording telephone conversations, meetings etc. within case notes if new information has been provided, including sources and dates;
- considering any challenges to the accuracy of the information and ensure that inaccuracies are corrected or inaccurate information is deleted in line with our Privacy Management Procedures;
- checking with the data source if any information is unclear and making sure the information recorded on our systems is entered accurately; and
- undertaking a regular audit of information assets to ensure that they are accurate and up to date.

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of

the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

This means that SCRA must:

- consider the purposes we hold the information for in deciding whether we retain it and for how long;
- only retain personally identifiable data for as long as is necessary;
- adopt suitable technical and organisational measures to prevent the reidentification of deidentified personal data.

We will comply with this principle by:

- utilising methods of pseudonymisation and anonymisation of data where appropriate;
- regular reviewing and destroying duplicate information held across the organisation; and
- securely disposing of information that is no longer needed or doesn't need to be retained in line with a legal requirement.

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This means that SCRA must:

- have appropriate technical (for example, system security) and organisational measures (for example, policies and procedures) in place to prevent personal data being accidentally or deliberately compromised, lost, destroyed or damaged;
- ensure the confidentiality, integrity and availability of the systems and services we use to process personal data;
- enable SCRA to restore access and availability to personal data in a timely manner in the event of a physical or technical incident; and
- ensure that we have appropriate processes in place to test the effectiveness of our measures, and undertake any required improvements.

We will comply with this principle by:

- designing our security to fit the nature of the personal data we process;
- adopting state of the art physical and technical security measures, supported by robust policies and procedures and well-trained staff;
- implementing robust Breach Management and Reporting Procedures;
- regularly reviewing information risks on SCRA's Strategic and Operational Risk Registers;
- ensuring that all staff (including temporary, secondments and contractors) undergo mandatory training on an annual basis; and
- implementing robust information security policies, access controls, security monitoring, and recovery plans.

2.2 Data protection law further requires that: **"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."**

This means that SCRA must:

- clearly document the lawful bases for processing personal data;
- document its processing activities;
- appoint a Data Protection Officer;

We will do this by:

- implementing appropriate data protection and information governance policies;
- taking a 'data protection by design and default' approach in the development of new systems;
- establishing data processing contracts with data processors;
- creating a Record of Processing Activities which includes details of all personal data processed by the organisation;
- implementing an Information Governance Framework which includes Privacy Management Procedures and guidance on data subjects rights under data protection law;
- regularly monitoring compliance with data protection law through a quarterly quality assurance framework;
- ensuring all staff receive bespoke annual training in the laws of data protection; and
- appointing our Information Governance Officer as SCRA's Data Protection Officer.

3. Lawful basis for processing

3.1 SCRA must have a valid lawful basis[3] in order to process personal data and we must determine and document that lawful basis before we begin processing.

3.2 When processing special category data[4] SCRA must identify a lawful basis for general processing and an additional condition[5] for processing this type of data.

3.3 When processing criminal conviction data or data about offences SCRA must identify a lawful basis for general processing and an additional condition[6] for processing this type of data.

3.4 If no lawful basis applies to the processing of personal data, special category data or criminal offence data, SCRA will be processing data unlawfully.

3.5 The lawful basis for processing can affect which rights are available to individuals. For further details please see our Guide to data subjects rights under data protection law.

3.6 SCRA will inform individuals of the lawful basis for processing data within SCRA's privacy notices as well as what rights individuals have in respect of the personal data processed. Records of the lawful basis for processing will be retained within the supporting documentation for our Record of Processing Activities.

[3] Please refer to the ICO guidance on determining the lawful basis for processing or Article 6 of the GDPR.
[4] For example, information about an individual's race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.
[5] Please refer to the ICO guidance on processing special category data or Article 9 of the GDPR.
[6] Please refer to the ICO guidance on processing criminal offence data or Article 10 of the GDPR.

4. Data subjects[7] rights

4.1 One of the key objectives of data protection law is to protect and strengthen data subjects rights in respect of the processing of their personal data. These rights include:

1. **The right to be informed**
2. **The right of access**
3. **The right to rectification**
4. **The right to erasure**
5. **The right to restrict processing**
6. **The right to data portability**
7. **The right to object**
8. **The right to not be evaluated on the basis of automated processing**

4.2 Further information in relation to each right, including how to exercise these rights and where exemptions may apply can be found in the Guide to Data Subjects Rights. Staff should also refer to the following Privacy Management Procedures:

Challenges to decisions based on automated processing
Data portability requests
Managing objections to data processing
Requests for data to be amended or rectified
Requests for data to be erased or deleted
Requests for data to be restricted
Subject Access Request Guidelines

4.3 All data subjects, regardless of age, have rights under data protection law. SCRA must consider the rights of all data subjects when considering data subjects rights, as listed above. For example, when considering a right of access by a parent in relation to their information and information relating to a child, SCRA must consider the rights of the child to protect their personal data when considering whether or not to release the information to a parent. SCRA must also be assured that the parent is acting on behalf of the child before releasing any information to them.

5. Data processors

5.1 Data protection law applies to both data controllers and data processors. SCRA is a data controller when we determine the purposes and means of processing personal data. If we ask a third party to process personal data on our behalf, they will be a data processor.

5.2 SCRA has a Data Processing Contract in place with each of its data processors, setting out the roles and responsibilities of the data processor in processing the data on SCRA's behalf.

5.3 SCRA is a data processor for Children's Hearings Scotland (CHS) in respect of HR and payroll processes. A Data Processing Contract is in place and details of the processing activities we carry out on behalf of CHS is documented within our Record of Processing Activities.

[7] A data subject is any individual whose personal data we process within SCRA, e.g. children, young people and families, staff, victims, witnesses, professionals.

6. Information sharing

6.1 Personal data should only be disclosed on a need to know basis and where there is a lawful basis for doing so. SCRA is required to share personal data in line with the requirements of the Children's Hearings (Scotland) Act 2011 and related rules. If SCRA receives a request from another individual or organisation for access to personal data outwith our statutory functions, staff should seek advice from the Information & Research Team.

6.2 Police officers or others requesting information for the purposes of a criminal investigation should be asked to put their request in writing. The request should include:

- what information is required
- why it is needed
- how the investigation will be prejudiced without it

This requirement can be set aside where the request is made in an emergency (i.e. a person is in immediate and imminent risk of serious harm).

7. International transfers

7.1 Personal data shall not be transferred to a country or territory outside the EU unless that country or territory ensures an adequate safeguards[8] in place to protect the rights and freedoms of data subjects in relation to the processing of personal data.

8. Roles and responsibilities

8.1 SCRA operates under the direction of a Board, which reflects a range of experiences and backgrounds in relation to children and young people. The Board plays a significant role in setting the strategic direction and in challenging and supporting SCRA to deliver its plans. Board Members have specific areas of responsibility linking to different areas of expertise and with different partners, such as Social Work Scotland and Police Scotland. The IG and data protection representative on the Board is Martin Toye.

8.2 SCRA's senior management meets monthly as the Executive Management Team (EMT) to discuss corporate direction and strategy, policy approval, corporate and operational planning and resourcing, organisational performance and corporate governance. It is the role of the EMT to have oversight of all data protection activities across the organisation and ensure that sufficient resources are provided to support compliance.

8.3 Information Governance Leads (IG Leads) have a key role in ensuring the security and effective management of SCRA's information to keep children safe. At a strategic level, the IG Leads influence and inform SCRA's data protection policies and practice, share good practice, highlight concerns and identify solutions. In localities, they champion good practice, and work with other managers to support staff and engage with partner agencies. It is the role of each IG Lead to act as the authority on IG in their locality and to be the main contact on IG and data protection issues.

[8] Please refer to the ICO guidance on assessing whether or not there are adequate safeguards in place when transferring data internationally.

8.4 The Head of Practice and Policy is SCRA's Senior Information Risk Owner (SIRO) – they are responsible for SCRA's IG Strategy and supporting IG Framework. They act as advocate for IG and data protection on the Executive Management Team and report to the Audit and Risk Committee on IG matters.

8.5 The Information and Research Manager and some members of the Information and Research Team are responsible for IG compliance across SCRA. They provide advice to staff in relation to IG matters, manage requests of data subjects in respect of their rights under data protection law and handle personal data breaches.

8.6 The Digital Governance Lead (DGL) reports to the Joint Head of IT (for CHS and SCRA) and is responsible for digital governance and security in SCRA.

8.7 The Information Governance Officer is SCRA's Data Protection Officer. It is their role to assist SCRA in monitoring internal compliance, informing and advising on data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting as a contact point for data subjects and the ICO. SCRA's DPO is tasked with monitoring compliance with data protection law, our data protection policies, awareness-raising, training, and audits.

8.8 Information Asset Owners (IAOs) are responsible for safeguarding our information assets and managing the associated risks. The IAOs in SCRA are senior managers and managers whose business areas use one or more registered SCRA Information Assets. Their role is to understand what information is held, what is added, what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to the information.. The IAOs are accountable to the SIRO, who in turn is accountable to the Principal Reporter who is our Accountable Officer (AO).

8.9 An IAO may appoint a Data Custodian to take on the daily responsibilities for managing an information asset on their behalf. The Data Custodian will ensure that the IAO is informed on how the asset is managed and will work with the IAO to mitigate any risks associated with the asset. The Data Custodian is also responsible for alerting the IAO of any incidents where the asset has been compromised or data has been lost so that necessary actions can be put in place to recover from the incident.

8.10 All staff within the SCRA are responsible for collecting, managing and sharing information appropriately and safely and in compliance with data protection law. It is the responsibility of all members of staff to ensure that they understand their role and responsibilities in relation to data protection. SCRA maintain evidence that their staff have understood their responsibilities through the completion of, or attendance at, annual training.

9. Legislative framework

9.1 Data protection activities are conducted in line with legislative and statutory requirements and best practice guidance, including:

EU General Data Protection Regulation
Data Protection Act 2018
Children and Young People (Scotland) Act 2014
HMG Security Policy Framework 2014
Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013
Children's Hearings (Scotland) Act 2011
The Retention of Samples etc (Children's Hearings) (Scotland) Order 2011

Public Records (Scotland) Act 2011
Environmental Information (Scotland) Regulations 2004
Criminal Justice (Scotland) Act 2003
Freedom of Information (Scotland) Act 2002
Human Rights Act 1998

10. Monitoring and Review

10.1 This policy will be reviewed every two years or as appropriate to take into account changes to legislation, and/or guidance from the Scottish Government or the UK Information Commissioner.

10.2 SCRA has introduced a locality self-assessment process for monitoring compliance with this policy and associated procedures and guidance. Quarterly, each locality and Head Office teams will complete the self-assessment and results will be reported to and considered by IG Leads.