INFORMATION GOVERNANCE – AN OVERARCHING FRAMEWORK

Document history, consultation and approval

Title	**SCRA Information Governance – An Overarching Framework**
Version	Version 1.2
Other relevant approved document	SCRA Data Protection Policy SCRA Records Management Policy SCRA Records Management Plan SCRA Information Governance Strategy SCRA Information Security Handbook SCRA Information Asset Owners Handbook SCRA Business Continuity Plan
Date of issue of policy	July 2012
Date of issue of this version	April 2019
Review date and by whom	April 2021 (To be reviewed at least bi-annually); Information Governance Leads Group
Prepared by	Information & Research Manager
Consultation	Information Governance Leads Group, EMT, Board Audit & Risk Committee
Approved by	Board Audit & Risk Committee

Table of Contents

Contact

For further information please contact:
Gillian Henderson
Information & Research Manager
Email: Gillian.henderson@scra.gsi.gov.uk

INFORMATION GOVERNANCE – AN OVERARCHING FRAMEWORK

1. Introduction

1.1 SCRA has statutory responsibilities as an organisation to the information it holds. This includes legislation governing use of personal information, principally the Data Protection Act 2018 (DPA) and EU General Data Protection Regulation (GDPR), Human Rights Act 1998, and Children's Hearings (Scotland) Act 2011. It also includes legislation governing wider information held by organisations, such as the Public Records (Scotland) Act 2011 (PRSA), and the Freedom of Information (Scotland) Act 2002 (FOISA).

1.2 SCRA also has accountabilities as a Non Departmental Public Body to Scottish and UK Governments. The Security Policy Framework (SPF) describes HMG's expectations of how public sector organisations and third parties handling citizen information and other information assets will apply protective security to ensure that they can function effectively, efficiently and securely. The Minimum Cyber Security Standard defines the minimum security measures that Departments (and public sector organisations) shall implement with regards to protecting their information, technology and digital services to meet their SPF and National Cyber Security Strategy obligations.

1.3 Information on children and families is essential for Reporter decision-making and the delivery of SCRA's service. SCRA as an employer has responsibilities for the information it holds on its staff. Information is also an asset - SCRA's statistical data and research influences and informs development of policy at local and national levels. The handling and security of information must be afforded the highest priority to safeguard those for whom we work and the organisation. Public confidence and trust in public authorities can be won or lost by the track record of a public body in managing information, especially highly sensitive, personal information.

2. Strategic aims

2.1 To continually improve SCRA's information governance and security to become a trusted leading public body in the management and governance of information.

To drive forward the improvement of information governance in SCRA so that:

- SCRA fully meets its statutory obligations for all personal information that it holds and processes.

- All SCRA staff understand their statutory and ethical obligations to personal information, and the individuals concerned.

- All SCRA staff treat others' personal information with the same respect they would expect for their own.

- SCRA meets its statutory obligations for records management of all the information it holds.

3. Scope

3.1 This framework covers all the information that SCRA holds in all formats, this includes:
- personal information related to children's cases and information on members of staff and Children's Panel Members
- aggregated statistical and research information
- financial information
- corporate information.

4. Statutory requirements and accountabilities

Data Protection Act 2018
4.1 SCRA is a Data Controller in terms of the DPA and GDPR. SCRA registers annually with the Information Commissioner's Office (ICO). Information on how SCRA processes personal data is provided on SCRA's web site: https://www.scra.gov.uk/contact-us/protecting-information/
Advice on how to request your personal information from SCRA is available at: https://www.scra.gov.uk/contact-us/requesting-information/

Freedom of information (Scotland) Act 2002
4.2 SCRA is listed in Schedule 1 of the FOISA. SCRA's Publication Scheme was approved by the Scottish Information Commissioner and is on SCRA's web site: https://www.scra.gov.uk/about-scra/freedom-of-information/ as is guidance on making a FOISA request.

Public Records (Scotland) Act 2011
4.3 SCRA is listed in the Schedule to the PRSA. SCRA's Model Records Management Plan has been approved the Keeper of the Records of Scotland, and is available on SCRA's web site: https://www.scra.gov.uk/about-scra/freedom-of-information/scras-model-publication-scheme/

Children's Hearings (Scotland) Act 2011
4.4 The Principal Reporter's powers to share information are largely defined by the 2011 Act and associated secondary legislation. The main powers of relate to investigation of referrals by the Reporter (section 66). Notifications which are prescribed in the Children's Hearings (Scotland) Rules and section 68 of the 2011 Act specify who can be notified of decisions of the Reporter.

Accountability to UK Government - HMG Security Policy Framework
4.5 SCRA, *via* Scottish Government, is accountable to UK Government for the security of its information assets. SCRA provides an annual return to Scottish Government on its compliance with the mandatory standards set by the

Security Policy Framework. A Data Processing Contract between the SCRA and the Information and Technology Services Division (iTECS) of the Scottish Government, was entered into in March 2019. The contract allows the SCRA to regulate the processing of certain personal data by iTECS.

Accountability to Scottish Government - Scottish Public Finance Manual
4.6 The Scottish Public Finance Manual (SPFM) requires that Accountable Officers of public bodies include a governance statement in their Annual Reports and accounts. Essential features of this governance statement are details of any significant lapses of data security and consideration of issues that may cause data integrity to be put at risk.

Staff information
4.7 SCRA is committed to ensuring that the personal information it holds on staff is held and managed in accordance with the legislation outlined above as well as complying with the ICO's Employment Practices Code. The Equality Act 2010, including both the general and specific duties, requires SCRA to gather and publish anonymised data on protected characteristics. This data is gathered during recruitment and selection exercises and staff in post are required to update their own data using self-service e-hr.

Statistical information
4.8 SCRA data and statistics are accredited as Official Statistics. This requires that statistical data are honest, objective and impartial; made available equally to all without cost to the end user with publishing dates openly announced far in advance.

Research information
4.9 Research conducted by SCRA and that of external researchers which requires SCRA resources must be approved in advance by SCRA's Research Ethics Committee.

5. Governance

5.1 SCRA's Board's Audit & Risk Committee is the accountable committee for information governance. An SCRA Board member has been assigned responsibility for information governance. Information Governance matters are listed as risks in SCRA's Operational Risk Register (December 2018) and Strategic Risk Register (December 2018) ; these are reviewed on a quarterly basis by the Executive Management Team (EMT) and six monthly by the Audit & Risk Committee.

5.2 The Information Governance Leads Group is accountable to the EMT in improving and managing SCRA's regulatory and statutory compliance for the personal data it holds and processes. The Group is Chaired by the Head of Practice & Policy. The Group's Remit and Role are attached at Appendix 1.

5.3 SCRA and Children's Hearings Scotland (CHS) as the key organisations in the Children's Hearings System established the CHS & SCRA Information

Governance Group. The Group's Terms of Reference are attached at Appendix 2.

5.4 The Head of Practice & Policy is the Senior Information Risk Owner (SIRO). There are Information Asset Owners (IAO) for each of SCRA major information assets and systems. The Information & Research Manager, Data Protection Officer, Digital Governance Lead, Personal Information Officer, Records Management Officer, and Information Assistant have specific responsibilities for information governance.

5.5 Information security and DPA compliance is included in the Job Descriptions of all operational managers (Locality Reporter Managers (LRMs) and Locality Support Managers) and is an appraisal objective of all LRMs.

5.6 Every member of SCRA's staff is responsible for the information they have access to and use. This is reinforced through annual mandatory Data Protection training and SCRA's Staff Code of Conduct.

6. SCRA policies and guidance

6.1 All SCRA staff must comply with SCRA's policies on information governance. Failure to do so is a breach of SCRA's Staff Code of Conduct.

- **Data Protection Policy** – provides the framework for SCRA on how personal information is processed, and aims to ensure compliance with the DPA. There is further guidance under this policy on specific areas including: managing and reporting data breaches, data subjects rights, Record of Processing Activities and Privacy Notices.

- **Information Sharing Guidance** - explains under what circumstances it is lawful to share information on children outwith the Principal Reporter's statutory powers.

- **Practice Direction 04 Non-Disclosure** and **2011 Act Non-Disclosure Operational Process and Guidance Note** set out how to deal with Non-Disclosure Order cases.

- **Records Management Plan** and **Records Management Policy** - set out how all information held by SCRA is managed. This includes the retention and disposal schedule.

- **Information Security Handbook** – sets out security requirements on electronic information. In addition, all staff as users of the Scottish Government's SCOTS network must comply with the SCOTS IT Code of Conduct.

SCRA INFORMATION GOVERNANCE LEADS GROUP

Remit

Information Governance Locality 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 Information Governance Leads influence and inform SCRA's policies and practice, share good practice, highlight concerns and identify solutions.   In Localities, they champion good information governance, and work with other managers to support staff and engage with partner agencies.

Role:

- Authority within Localities on information governance

- Main contact in Locality to provide advice and support to Locality staff on information governance issues

- Main Locality link to Data Protection Officer

- Work as a team with the other Locality Information Governance leads and Data Protection Officer to share experience and good practice

- Lead on subject access requests in Locality

- Lead on records management in Locality

- Work with and support other Locality managers in working with partner agencies to improve information governance across the Children's Hearings System.

Agreed – September 2013

CHS AND SCRA INFORMATION GOVERNANCE GROUP

TERMS OF REFERENCE

1. Purpose

1.1 To consider information governance[1] (IG) and complaints issues affecting CHS and SCRA, to share knowledge and experience, to highlight IG issues that affect the Children's Hearings System and to progress improvements in IG and complaints handling in both organisations.

2. Aim

2.1 The aim of the group is to improve IG across both organisations, ensure best practice and effective IG in the operation of children's hearings and identify opportunities for partnership working.

3. Scope

3.1 The remit of the IG Group will be to discuss common areas of interest and responsibility as well as IG related concerns, queries and experiences. These will include but not be limited to:

- Information security incidents, vulnerabilities and threats
- Relevant complaints affecting both organisations
- Internal/external audits
- Data controller and data processor relationships
- Relevant legislative and statutory requirements in relation to IG
- Information sharing opportunities and responsibilities
- Panel member contact details
- Security of panel papers
- Training
- Lessons learnt

3.2 The group will also consider any opportunities to carry out peer reviews of policies, procedures, training etc.

4. Membership

4.1 Group meetings will usually be attended by the following staff from each organisation, however, the membership is flexible and is open to anyone who wishes to attend from either organisation:

---

[1] Information Governance issues include those relating to Data Protection, Freedom of Information, information security, information sharing and records management.

SCRA   Head of Practice & Policy
*   Information and Research Manager*
*   Data Protection Officer*
*   Locality Support Manager*

CHS   Director of Finance and Corporate Services / Senior
*   Information Risk Owner*
*   Information Governance Officer*
*   Performance and Research Officer*
*   Panel and Area Support Officer*

4.2   A minimum of 2 staff (1 from each organisation) must be present for a meeting to proceed.

5.   Meetings

5.1   Meetings will take place at CHS's premises in Edinburgh and will be chaired by either CHS's Information Governance Officer or SCRA's Information and Research Manager, on an alternate basis. The first meeting is scheduled for 28 January 2015.

5.2   The group aims to meet at least four times per year on a quarterly basis. Additional meetings will be scheduled if there are specific concerns or issues that require earlier discussion.

5.3   Agenda items will be agreed and issued two weeks in advance of meetings by the Chair of   the next meeting. Minutes will be taken by either CHS's Information Governance Officer or SCRA's Information and Research Manager, on an alternate basis.

6.   Accountability

6.1   CHS group members will report to the National Convener / Chief Executive Officer and the Audit and Risk Management Committee.

6.2   SCRA group members will report to the Principal Reporter / Chief Executive Officer, the Senior Information Risk Owner and the Information Governance Leads Group.

Agreed – October 2014