SCOTTISH

CHILDREN'S REPORTER

ADMINISTRATION

SCRA RECORDS MANAGEMENT POLICY

Document history, consultation and approval

Title	**SCRA Records Management Policy**
Version	Version 1.4
Other relevant approved document	Information Governance Overarching Framework Case Information Policy Information Security Handbook
Date of issue	21 March 2011
Review date and by whom	Revised following: EMT comments– December 2010 ICO Audit recommendations and SCRA Action Plan – August 2014 To be reviewed at least annually
Prepared by	Information & Research Manager
Consultation	EMT, Information Governance Leads,
Approved by	EMT

Table of Contents

Contact

For further information please contact:

Gillian Henderson
Information & Research Manager
Email: Gillian.henderson@scra.gsi.gov.uk
Tel: 0300 200 1573

1. Introduction

Records management is essential to the delivery of our service in an efficient and accountable manner, and to ensure that we meet our statutory requirements.

SCRA believes that effective records management will bring many benefits. It will make savings by reducing time spent searching for and retrieving records and it will reduce storage costs. It will improve our performance by reducing duplication, improving consistency of information and advice, and providing ready access to information on SCRA policies, practice, decisions and governance.

What is records management[1]?

Records management is the practice of formally managing records within a file system (electronic and/or paper) including classifying, capturing, storing and disposal.

A **record** is information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

Statutory requirements

As a public body SCRA is required by law to manage its records properly. Legislation such as the Data Protection Act 1998[2] and the Freedom of Information (Scotland) Act 2002[3] set out specific requirements in relation to the creation and management of records.

The Public Records (Scotland) Act 2011 is the main legislation governing Scottish Public Records. SCRA is a named public authority in the Act and is obliged to prepare and implement a records management plan (RMP) which sets out proper arrangements for the management of its records. The RMP will be agreed with the Keeper of the Records of Scotland in 2015 and is to be regularly reviewed. Where authorities fail to meet their obligations under the Act, the Keeper has powers to undertake records management reviews and issue action notices for improvement.

Scope of this policy

This policy sets out how ALL SCRA records are to be managed. Personal information on staff members is covered by SCRA's Employment Records Management Policy and Procedures. Personal information related to

[1] The National Archives' definitions.
[2] Specifically the fifth Data Protection Principle – 'Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposees'.
[3] Code of Practice for public authorities on the discharge of their functions under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004.

children's cases is covered by SCRA's Case Information Policy. The security of SCRA's information is covered by the Information Security Handbook.

2. Policy principles[4]

This policy requires that all SCRA staff work in accordance with the following information management principles:

- SCRA's information is a **corporate resource**, and not 'owned' by any individual.
- **Personal responsibility** – each one of us is personally responsible for the effective management of the information we create or use.
- **Information accessibility** – we make our information accessible to others in SCRA, except where there is a specific and agreed reason not to.
- **Keeping records of what we do** – we retain records of all the decisions and actions we make; we maintain an audit trail to meet business, regulatory and legal requirements; we track policy changes and development.
- **Ensuring information is accurate and fit for purpose** – we ensure that the information we create on behalf of SCRA is accurate and fit for purpose.
- **Compliance with statutory and regulatory requirements** – we ensure that our information management practices comply with all relevant statutory and regulatory requirements.
- **Electronic records** – use of paper records will be minimised. All documents and information will be held electronically unless there is a requirement for a paper record.

3. Who does this policy apply to?

This policy applies to ALL SCRA employees and contractors who have access to our records.

Responsibility for the standard, accuracy and completeness of SCRA records and how this information is used on a daily basis lies with individual members of staff. This means that everyone with access to SCRA records does so in accordance with this policy.

4. What does this policy apply to?

This policy apples to the management of all records (paper, electronic, or other media) created or received by SCRA. This includes:

- Documents (hand written, typed, and annotated copies);
- Computer files (including databases, spreadsheets and presentations; and systems such as iTrent and Cedar);
- Paper based files;

[4] Based on the Scottish Government's Information Management Principles

- Case Management System
- Data Warehouse
- Electronic mail messages and their attachments;
- Diary records;
- Reports; and
- Intranet and internet web pages.

5. Records retention

SCRA records should be held and retained according to the Records Retention Schedule (page 7, and Annex 2 for employment records). This categorises records according to function, sets out how long records should be kept before being destroyed, and how they should be marked to determine how they should be held and used. Retention periods are based on existing SCRA retention policies (where these exist) and on those used by partners such as Scottish Government, ACPOS and COPFS.

The Records Retention Schedule applies retrospectively.

Disposal

Records should be destroyed according to their Government Security Classification marking. All **OFFICIAL** and **OFFICIAL-SENSITIVE** data must be disposed of as confidential waste[5].

[5] Details on the disposal of OFFICIAL and OFFICIAL SENSITIVE data are in Appendix E of the Information Security Handbook

6. Records retention schedule[6]

Function	Record description	Retention action		Responsibility	Marking
		Disposal	**Legislative and policy requirements**		
Audit	Practice Audit	Reports – 6 years Paperwork – current year + 3		Head of Planning & Strategy; Director of Support Services	OFFICIAL
Audit	Internal and external audit	Reports – 6 years Paperwork – current year + 3	Companies Act 2006	Director of Support Services	OFFICIAL
Children's case information	Case Management System and hard copy files	Until child reaches 18 years (unless exception applies)	Case Information Policy, Retention of Case Information After 18th Birthday (to meet obligations under Criminal Justice & Licensing (Scotland) Act - re. forensic data); Guidance on Retention of Paper Files	Director of Support Services, Head of Practice & Policy	OFFICIAL

[6] HR records should be retained according to Employment Records Retention Schedule at Annex 2.

Communications	Staff communications	Current year + 1		Press & Communications Manager	Not protectively marked
Communications	Publications	Material not published – current year + 1		Press & Communications Manager	Not protectively marked
Complaints	Correspondence and associated records	Current year + 6	Case Information Policy; Retention of Case Information After 18th birthday	Director of Support Services	OFFICIAL
Contract Management	SCOTS contract, etc.	5 years after closure		Head of Finance and Resources, IS Manager,	OFFICIAL
Data Management	Data reports	If not published, current year + 5	Case Information Policy; Retention of Case Information After 18th Birthday.,	Data Manager	Not protectively marked unless information on individuals – OFFICIAL-SENSITIVE.
Data Management	Databases (workload, FOISA requests, data requests)	Current year + 5	Case Information Policy; Retention of Case Information After 18th Birthday	Data Manager	Not protectively marked unless information on individuals – OFFICIAL -SENSITIVE.
Data Management	Data Warehouse development, licence/support documentation,	Current year + 5 or until superseded		Data Manager	Not protectively marked

	processes and controls				
Finance	Financial transactions (e.g. invoices (debtors and suppliers), requisitions, GPC logs, forecast outturns)	Current year + 6 (statutory requirement)	Companies Act 2006	Finance Assistant, Business Managers, GPC holders	OFFICIAL
Finance	Budget management (e.g. annual budget, annual accounts, Balance sheet reconciliations	Current year + 6 (statutory requirement)	Companies Act 2006	Head of Finance and Resources	OFFICIAL
Finance	Asset management (asset register, disposals, transfers, etc.)	Current year + 6 (statutory requirement)	Companies Act 2006	Finance Assistant, IS Manager	OFFICIAL
Finance	Falkirk Council Pension Fund investment Forum related papers and correspondence	Current year + 1 (statutory requirement)	Retirement Benefits Schemes Regulations 1995	Head of Finance and Resources	OFFICIAL
Finance	Grant in Aid drawdown requests	Current year + 10		Head of Finance and Resources	OFFICIAL
Finance	HMRC correspondence	Current year + 5	Income Tax (Employments) Regulations 1993	Head of Finance and Resources	OFFICIAL
Finance	Finance journals	Current year + 6 (statutory requirement)	Companies Act 2006	Head of Finance and Resources	OFFICIAL
General	Correspondence	Current year + 3		All	Not protectively marked
General	Meetings (internal and external) not listed above	Current year + 5		All	Not protectively marked
General	Reference materials	Current year + 5		All	Not protectively marked
Governance	Board (and its Committees) meetings, agendas, papers minutes	Current year + 10		Executive Officer	OFFICIAL
Governance	EMT meetings, agendas, papers minutes	Current year + 5		Executive Officer	OFFICIAL
Governance	Partnership Forum meetings, agendas, papers minutes	Current year + 10		Director of Support Services	OFFICIAL
Governance	Strategic Risk Register	Current year + 10		Head of Finance and	OFFICIAL

				Resources	
Governance	Relations with Scottish Government inc. Framework documents	Current year + 10		Executive Officer	OFFICIAL
Governance	Strategic planning inc. Programme Board	Current year + 10		Head of Planning & Strategy	Not protectively marked
Governance	Spending Reviews	Current year + 10		Head of Finance and Resources	OFFICIAL
Information management	Freedom of Information requests and responses, and associated records	Current year + 3		Information & Research Manager	Not protectively marked unless information on individuals – OFFICIAL-SENSITIVE
Information management	Data Protection enquiries inc. Subject Access Requests	Current year + 3	Case Information Policy	Information & Research Manager,	OFFICIAL-SENSITIVE
Information management	PVG requests from Disclosure Scotland	Current year + 3	Case Information Policy; Protection of Vulnerable Groups Act	Information & Research Manager	OFFICIAL-SENSITIVE
Information management	Information security breaches inc. Non-Disclosure	Until child reaches 18 years (unless exception applies)	Case Information Policy; Practice Direction 4; Retention of Case Information After 18th Birthday	Information & Research Manager	OFFICIAL- SENSITIVE
Information Management	Compliance – information security, data protection, etc.	Policies and technical documentation – until superseded Other – current year + 3		IS Manager	Not protectively marked

IS	Systems inc. CMS	Current year + 1 (unless related to contracts)		IS Manager	OFFICIAL
IS	Telephony	Current year + 1 (unless related to contracts)		IS Manager	Not protectively marked
IS	Maintenance	Current year + 1 (unless related to contracts)		IS Manager	Not protectively marked
Media	Daily press cuttings	One month		Press & Communications Manager	Not protectively marked
Media	Media tracker and enquiries	Current year + 6	Case Information Policy	Press & Communications Manager	OFFICIAL
Media	Press statements, media related correspondence	Current year + 6		Press & Communications Manager	Not protectively marked
Organisational Development	IIP, workforce planning, etc.	Current year + 5		Director of Support Services	OFFICIAL
People Management	Team meetings, training plans, team plans, team budgets, etc.	Current year + 1		Team managers	Not protectively marked
Performance Reporting	Annual Reports, OPR, KPIs, etc.	If not published – current year + 5		Head of Planning & Strategy	Not protectively marked
Performance Reporting	Performance analysis reports	If not published, current year + 5		Head of Planning & Strategy	Not protectively marked
Planning	EFQM, etc.	Current year + 5		Head of Planning & Strategy	Not protectively marked
Planning	Corporate, Business and Locality plans	Current year + 5		Head of Planning & Strategy	Not protectively marked
Policy	Scottish Parliament	Current year + 5		Policy & Public Affairs Manager	OFFICIAL
Policy	Scottish Government	Current year + 5		Policy & Public Affairs Manager	OFFICIAL;
Policy	Policy and legislative development	Current year + 5		Policy & Public Affairs Manager	OFFICOAL
Practice	Memorials for the Opinion of Counsel and the resulting Counsel's Opinion	To be reviewed after current year + 10		Practice Manager	OFFICIAL-SENSITIVE

		Held securely, with limited access.			
Practice	Court activity	Until child reaches 18 years (unless exception applies)	Case Information Policy; Retention of Case Information After 18th Birthday	Practice Manager	OFFICIAL-SENSITIVE
Practice	Enquiries received *via* Practice Helpline	To be reviewed after current year + 10 (unless exception applies)	Case Information Policy	Practice Manager	OFFICIAL-SENSITIVE
Practice	Child death reports	Destroyed when SCRA notified of child's death unless required for further investigation or an enquiry (e.g. Fatal Accident Inquiry, Significant Case Review, etc.). Retention of these records must be reviewed at least annually. Held securely, with limited access.	Case Information Policy; Practice Instruction Note 10	Head of Practice & Policy	OFFICIAL-SENSITIVE
Procurement	Tender exercises	5 years after closure		Head of Finance and Resources	OFFICIAL
Procurement	Approved suppliers and frameworks	5 years after closure		Head of Finance and Resources	OFFICIAL
Project Management	Project plans, business cases, business plans change control notes, progress reports, project closure reports etc.	6 years after completion of project Working documents – current year + 1	Companies Act 2006	Head of Planning & Strategy	Not protectively marked
Property	Maintenance of SCRA estate	Current year + 10	Companies Act 2006	Head of Property	OFFICIAL

Property management	Information related to ownership, statutory consents, etc.	For as long as SCRA holds the property	Companies Act 2006	Head of Property	OFFICIAL
Property management	Property management records	Current year + 10	Companies Act 2006	Head of Property	OFFICIAL
Research	Information and materials gathered for research	On completion Held securely, with restricted access	Case Information Policy	Information & Research Manager	OFFICIAL-SENSITIVE
Research	Research not otherwise published	Current year + 5		Information & Research Manager	Not protectively marked
Surveys	Staff and partners	Reports - current year + 6 Collated data – current year +1 Individual returns - held securely, restricted access		Press & Communications Manager	Reports – not protectively marked. Individual returns - OFFICIAL
Training	Training materials –inc. Practice Training	Destroy when superseded Other – current year + 1		Head of Practice & Policy, Learning & Development Manager	Not protectively marked

Government Security Classifications (GSC)[7]

The Government Security Classifications that were introduced on 2 April 2014 offer three levels of classification:-

- TOP SECRET
- SECRET
- OFFICIAL

The majority of information that is created or processed by the public sector is to be classified at the OFFICIAL level, some of which could have damaging consequences if lost stolen or published in the media, but are not subject to a heightened threat profile.
OFFICIAL SENSITIVE is a subset of the OFFICIAL classification which is to be used for particularly sensitive information and should be managed within the OFFICIAL classification tier.

Government Protective Marking Scheme (GPMS)

The Government Protective Marking Scheme is being replaced by GSC. GPMS was recognised by SCRA previously and is still in use by some public sector organisations. GPMS offers 5 levels of classification :-

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED
- PROTECT

The term "UNCLASSIFIED" or "NOT PROTECTIVELY MARKED" is commonly used to indicate that a GPMS protective marking is not needed.

Protective Marking using GSC

For particularly sensitive information requiring a more limited 'need to know' level of protection then a **caveat** is used by protectively marking the information **OFFICIAL–SENSITIVE**.
There is no requirement to explicitly mark routine OFFICIAL information**.**

Handling Descriptors using GSC

Applying a **handling descriptor** to the protective marking makes the need for protection clearer and is added to the **OFFICIAL–SENSITIVE** protective marking. There are 2 descriptors that are currently in use by SCRA, these are:

- COMMERCIAL – commercial or market sensitive information
- PERSONAL – sensitive information relating to an identifiable individual

e.g. **OFFICIAL–SENSITIVE PERSONAL**
expected to understand the data classification policy and how it applies to the information assets that they handle.

[7] From SCRA's Data Classification Policy v1.0 in Information Security Handbook

OFFICIAL	It becomes OFFICIAL- SENSITIVE when…
All records which allow people to be identified are “personal data” and we are trusted to protect it.	…children or vulnerable adults may be at direct risk of harm if the information is shared with the wrong people.
Management information and reports are critical to smooth running and accountability of the business.	…announcements or processes associated with it would be seriously harmed if released.
Draft reports are protected before released to the public.	…the content is so controversial that mishandling will have serious consequences for SCRA or Scottish Government.
Information Technology network plans might be commercially sensitive or contain details of security controls in place.	…indicated security vulnerabilities would allow an attacker to seriously compromise our systems.
Policy development and advice to ministers.	…if the subject is very contentious and sensitive

Table 1: Routine business information and sensitive business information

Annex 2

EMPLOYMENT RECORDS MANAGEMENT POLICY AND PROCEDURES

1. Statutory Requirements

In addition to those on page 4, SCRA will comply with:

- The Information Commissioner's Employment Practices Data Protection Code Part 2: Employment Records
- Other relevant statutory standards (e.g. Finance)
- Best practice (e.g. from Chartered Institute of Personnel & Development).

2. Access to Personal Files

Individual current and former employees have a right to access information kept regarding them. There are some exemptions which are outlined at section 3.

If an employee requests to see their personal file the following points should be adhered to by the data controller:

1. Inform the employee of the information kept about him or her, giving a description of it, the purposes it is kept for and any organisations which it may be passed onto (if any).

2. Show the employee all the information SCRA keeps regarding him or her, explaining all codes or other cryptic terms.

3. Information should be provided on hard copy or in readily readable permanent electronic form unless providing it in that way would involve disproportionate effort or the employee agrees to receive it in some other way.

4. Provide the employee with any additional information SCRA has as to the source of the information kept about him or her.

SCRA will provide access to personal information within 40 calendar days of receipt of a written request. Personal files should be viewed in the Human Resources team or relevant Regional HQ offices.

It is the responsibility of the data controller to inform relevant managers, or other staff, of the nature of the information being released if it may affect them in some way.

3. Exemptions to the Right to Access Personal Information

There are a number of exemptions to the right to access personal information which are relevant to personal files. They are:

1. Information held for management forecasting or workforce planning (for example, plans to promote, transfer or make an individual redundant).

2. Information detailing the intentions of the employer in relation to negotiations with a worker may be withheld to the extent to which access would be likely to prejudice those negotiations, for example because it would give away the employer's 'fall-back position'.

3. References given, or to be given, by SCRA for:
   - the education, training or employment of the worker
   - the appointment of the worker to any office
   - the provision by the worker of any service.

   may be withheld, although it is SCRA practice to provide employees with a copy of any reference given to external organisations or in connection with internal applications.

4. Information held for:
   - the prevention or detection of crime
   - the apprehension or prosecution of offenders
   - the assessment or collection of any tax or duty or of any other imposition of a similar nature.

   may be withheld to the extent to which access would be likely to prejudice any of these matters.

5. Access to information involving third parties is subject to exemptions. It is the responsibility of the data controller to make a judgement as to what information is reasonable to withhold concerning the identification of a 3rd party as such identification would violate the rights of the 3rd party. For example if a complaint was made about the data subject it would be sensible to remove the identity of the 3rd party in this instance. However if the identity of the 3rd party remains obvious then it is at the discretion of the data controller to consider withholding this information altogether in order to respect the rights of 3rd party privacy.. If the 3rd party consents to disclosing the information SCRA may disclose it to the data subject. Advice should be sought from SCRA's HR Business Partners to assist with such decisions.

4. Providing 3rd Party Organisations with Personal Data

SCRA's Responsibilities

SCRA may outsource a number of its functions to 3rd party organisations (for example, pension schemes). SCRA is also responsible for taking all reasonable steps to ensure that the 3rd party organisations will treat the data with due care and respect. SCRA must not use information given for a particular purpose by an individual for any different purpose. Permission must be granted by the individual to do so.

5. Employment Records Retention Schedule

No.	Record description	Storage Medium* (Paper/ Electronic/Both)	Retention action		Responsibility	Marking
			Disposal	**Other requirements**		
1.	**Recruitment**					
1.1	Job descriptions	Electronic	Destroy 5 years after creation		HR Manager	Not protectively marked
1.2	Individual job description on personal file Successful candidates: application form, CV, offer and acceptance letters	Electronic	Destroy 6 years after employment ceases		HR Manager	Not protectively marked
1.3	Grading of individual jobs: outcomes	Electronic	Destroy 10 years after superseded		HR Manager	Unmarked
1.4	Vacancy authorisation form/authorisation of recruitment	Electronic	Destroy 5 years after completion of recruitment		HR Manager	Official
1.5	Advertising details	Electronic	Destroy not less than 3 years after the financial year into which they relate		HR Manager	Not protectively marked
1.6	Advert text	Electronic	Destroy immediately after job description is superseded		HR Manager	Not protectively marked
1.7	Disclosure Scotland or equivalent tracking sheet	Electronic	Following full SCRA review		HR Manager	Official
1.8	Unsolicited applications and the SCRA's reply	Electronic	Destroy immediately		HR Manager	Official

* Record may currently be stored in paper format but should be transferred to the following storage format where possible.

1.9	Records documenting enquiries about vacancies and requests for application forms unsuccessful candidates: application forms, CVs, references, interview notes.	Electronic	Destroy 6 months after completion of recruitment		HR Manager	Official
1.10	Occupational testing documents	Electronic	Destroy test results for all internally and externally appointed candidates after 24 months. Destroy unsuccessful candidates after 6 months.		HR Manager	Official
1.11	Equal opportunities form	Electronic	Destroy immediately after information is entered onto database		HR Manager	Official
1.12	Equal opportunities database information	Electronic	Destroy 10 years after information is entered onto database		HR Manager	Official
1.15	Copies of passports and identity cards	Electronic	Destroy non EEA and Swiss records after 6 months. Retain other until become British Citizen or 12 months after leaving		HR Manager	Official

2	**Staff development, conference attendance, training & induction**					
2.1	Records arising from the identification of staff development needs on a departmental or SCRA-wide basis, including the development of plans to meet those needs	Electronic	Destroy 5 years after creation		Learning & Development Manager	Official
2.2	Records documenting the development, overall delivery and assessment of induction or other training programmes, including feedback analysis	Electronic	Destroy after current year +2 years		Learning & Development Manager	Official
2.3	Training records relating to individuals	Electronic	Destroy 6 years after employment ceases		Learning & Development Manager	Official
2.4	Institute of Leadership and Management (ILM) candidate records	Electronic	Destroy 5 years after completion of course module		Learning & Development Manager	Official
3	**Remuneration and reward**					
3.1	Records documenting the development of SCRA's remuneration structure and strategy and pay reviews Records documenting an employee's remuneration and rewards.	Electronic	Destroy 6 financial years after the record created	Taxes Management Act 1970	HR Manager	Official
3.2	SCRA's salary placement policy	Electronic	Destroy 6 financial years after the policy created	Taxes Management Act 1970	HR Manager	Not protectively marked

4	**Grievances**					
4.1	Records documenting grievances raised by staff, SCRA's response, action taken and the outcome.	Electronic	Destroy 6 years after last action on file		HR Manager	Official
5	**Employee contract management**					
5.1	Contract, offer letter and amendment to terms and conditions documentation. Immigration paperwork Records documenting changes to an employee's terms and conditions of employment.	Electronic	Destroy 6 years after employment ceases	Taxes Management Act 1970	HR Manager	Official
5.2	Records arising from the appraisal process or otherwise recording an employee's training and development needs, and the action taken to meet these needs. Records documenting routine assessments of an employee's performance, and any consequent action taken.	Electronic	Destroy after 4 years		Line manager	Official
5.3	Records documenting disciplinary proceedings against an employee.	Electronic	Destroy 6 or 12 months after warning lapses		HR Manager	Official

5.4	Records documenting job-specific statutory/regulatory training requirements for an employee (e.g. health and safety training or fire safety training for fire wardens), and the training provided to meet these requirements.	Electronic	6 years after employment ceases		Learning & Development Manager	Official
5.5	Records documenting the authorisation and administration of annual, floating public or special leave.	Electronic	Destroy after current year + 1 year		Line manager	Official
5.6	Records documenting the authorisation and administration of statutory leave entitlements, e.g. parental leave.	Electronic	Destroy after completion of entitlement or current year +1 whichever is greater		HR Manager	Official
5.7	Records documenting entitlements to, and calculations of, Statutory Maternity Pay.	Electronic	Destroy after current tax year + 3 years	Statutory Maternity Pay (General) Regulations 1986, as amended	HR Manager	Official
5.8	Records containing an employee's current basic personal details (e.g. address, next of kin, emergency contacts).	Both All info on HR/Payroll System Emergency contact info only paper.	Retain information on HR & OD database and contact details on paper for current employees		HR Manager Line Manager	Official

5.9	Records documenting an employee's termination of employment Exit interview notes and analysis	Electronic	Destroy 6 years after termination of employment		HR Manager	Official
5.10	References provided in support of an employee's application(s) for employment by another organisation.	Electronic	Destroy 6 years after provision of reference		HR Manager	Official
6	**Sickness**					
6.1	Records documenting an employee's absence due to sickness.	Both	Destroy paper Current tax year + 3 years Retain HR system record indefinitely.	Statutory Sick Pay (General) Regulations 1986, as amended	HR Manager	Official
6.2	Referrals to Occupational Health Providers by self or manager	Both	Destroy 10 years after last treatment, patient's death or permanent removal from the country.		HR Manager	Official
7	**Health & Safety**					
7.1	Records documenting the issue of personal protective equipment/other special equipment to an employee.	Both	Destroy 6 years		H&S Adviser	Official
7.2	Health surveillance regarding staff exposed to hazardous substances including biological agents	Both	Destroy date of last entry plus 40 years	The Control of Substances Hazardous to Health Regulations 1999 and 2002	H&S Adviser	Official

7.3	Records documenting accident, incidents, diseases and dangerous occurrences to adults and children	Both	Destroy date of last entry -plus 3 years (accidents, incidents & dangerous occurrences) -plus 40 years for diseases (employees)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995, as amended. Limitation Act 1980 The Control of Substances Hazardous to Health Regulations 1999 and 2002	H&S Adviser	Official
7.4	Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	Both	Destroy 5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 and 2002	H&S Adviser	Official
7.5	General health surveillance records for staff	Both	Destroy date of last surveillance plus 40 years	The Control of Substances Hazardous to Health Regulations 1999 and 2002	H&S Adviser	Official
7.6	Flexi sheets	Both	2 years after sign off		Line manager	Official
7.7	Assessments under Health and Safety Regulations and records of consultations with safety representatives	Both	Retain permanently		Line manager	Official

	and committees					
8	**HR Policies**					
8.1	HR policies: master copy	Electronic	Destroy 5 years after policy is superseded		HR Manager	Official
8.2	HR policies	Electronic	Destroy immediately when no longer required for departmental/personal reference		HR Manager	Official

9	**HR Procedures**					
9.1	HR procedures and guidance Interpretation of procedures or guidance at local or central level	Electronic	Destroy 2 years after guidance is superseded		HR Manager	Official
10	**Job Evaluation**					
10.1	Working papers from job evaluation exercises	Electronic	Destroy 1 year after completion of exercise		HR Manager	Official
10.2	Results of job evaluation exercises	Electronic	Destroy 10 years after completion of exercise		HR Manager	Official
11	**Pension schemes administration**					
11.1	Actuarial valuation reports	Both	Permanently retain		Finance Manager	Official
11.2	Records documenting the institution's relationships with pension schemes to which all or part of its workforce belongs	Both	Destroy 5 years after relationship with pension scheme ceases	The Retirement Benefits Schemes (information Powers) Regulations 1995	Finance Manager	Official
11.3	Routine communications with the pension schemes	Electronic	Destroy 5 years after creation	The Retirement Benefits Schemes (information Powers) Regulations 1995	Finance Manager	Official
11.4	Records of individual employees' pension contributions and entitlement	Electronic	Destroy 40 years after creation or on death of member's beneficiary - whichever is the greater		HR Manager	Official
11.5	Pension scheme investment policies		Destroy 12 years from the last benefit payable		Finance Manager	Official

			under the scheme			
11.6	Records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents: All retirement records including papers created by SCRA, pension providers, occupational health providers or legal advice given.	Both	Destroy 6 years from the end of the scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed.	Retirement Benefits Schemes (Information Powers) Regulations 1995	HR Manager	Official
12	**Payroll**					
12.1	Senior executives' records (that is, those on a senior management team or their equivalents) Inland Revenue approvals	Electronic	Permanent		HR Manager	Official
12.2	Income tax and NI returns, income tax records and correspondence with the Inland Revenue Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	Electronic	Destroy not less than 3 years after the end of the financial year to which they relate	The Statutory Maternity Pay (General) Regulations 1986, as amended	HR Manager	Official
12.3	Relocation expenses claims	Electronic	Destroy 3 years after appointment		HR Manager	Official

12.4	Wage/salary records (also overtime, bonuses, expenses): overtime documentation and sign off, payroll amendments (NOT contractual letters or offers of employment). Redundancy details, calculations of payments, refunds, notification to the Secretary of State	Electronic	Destroy current financial year + 6 years	Taxes Management Act 1970	HR Manager	Official
12.5	Mortgage/Credit requests	Electronic	Destroy Three months after sharing copy with individual		HR Manager	Official
12.6	Electronic & paper payslips Electronic & paper payroll reports	Electronic	Destroy after auditors have visited and assessed previous financial year		HR Manager	Official
12.11	Payroll exception reports and reconciliations as per payroll procedures	Electronic	Destroy 1 year after current financial year		HR Manager	Official

Definitions

Sensitive Data - any information which relates to (for the purposes of this policy): race or ethnic origin, political opinions, religious beliefs or other beliefs of similar nature, trade union membership, physical or mental health condition, including disabilities, sexual orientation, any information regarding an individuals offence/s committed, or allegedly committed.

Personal Data - that which relates to a living person and identifies an individual, either on its own or together with other information that is in SCRA's possession, or that is likely to come into its possession.

Data Subject - an individual who is the subject of personal data.

Data Controller - a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed. A legal entity itself can be determined a 'controller' or an individual within it.