SCCYP

Scotland's Commissioner for Children & Young People

Records Management Plan

April 2015

Prepared in accordance with the Public Records (Scotland) Act 2011 and submitted to the Keeper of the Records of Scotland for their agreement on 28 April 2015

(Revised and submitted on 19 August 2015)

Contents

Commissioner's Statement

The Public Records (Scotland) Act 2011 promotes efficient and accountable record keeping by Scottish public authorities. It requires an authority to produce and implement a records management plan; this plan should clearly describe the way an authority cares for the records they create, in any format, as they carry out their functions and duties.

As a named authority, this plan has been prepared to establish a framework for the management of public records within the office of Scotland's Commissioner for Children and Young People. I recognise the value of our records; they are our corporate memory, providing evidence of the actions and decision making that underpins our daily functions and operations, helping us to promote and safeguard the rights of children and young people in Scotland.

This plan will be implemented and kept under regular review to improve the quality of record keeping within my office. The plan identifies a number of gaps in the provision of good records management; however it does make firm commitments to address them.

My staff and I are committed to establishing effective records management arrangements, aware that in doing so we will deliver significant benefits for the office. Good records management will allow us to increase our overall efficiency and effectiveness, support our decision making processes and enable us to meet our statutory obligations, particularly as laid down by the Freedom of Information (Scotland) Act and the Data Protection Act.

Tam Baillie,
Scotland's Commissioner for Children and Young People

Element 1: Senior Management Responsibility

Element 1: Senior Management Responsibility	
Element Requirement	This is a compulsory element of the Public Records (Scotland) Act 2011. Identify an individual at senior level who has overall strategic accountability for records management.
Statement of Compliance	The individual at senior level who has overall strategic accountability for records management is Stephen Grounds, Head of Corporate Services. Stephen Grounds is one of the Commissioner's three Heads of Department; the Heads of Department sit on the Management Team along with the Commissioner.
Evidence of Compliance	Evidence submitted in support of Element 1 comprises: • **Evidence 1.1:** Letter from Head of Corporate Services supporting elements 1, 2 and 3. • **Evidence 3.1:** Information and Records Management Policy (section 5: roles and responsibilities).
Action Required	No further action is required in respect of Element 1.

Element 2: Records Manager Responsibility

Element 2: Records Manager Responsibility	
Element Requirement	This is a compulsory element of the Public Records (Scotland) Act 2011. Identify an individual within the authority, answerable to senior management, to have day-to-day operational responsibility for records management within the authority. It is vital that an authority's records management plan confirms that an individual has been appointed to have overall day-to-day responsibility for the implementation of the plan.
Statement of Compliance	The individual answerable to senior management with day-to-day operational responsibility for records management is Gillian Munro, Information Officer. Gillian reports to Stephen Grounds, Head of Corporate Services.
Evidence of Compliance	Evidence submitted in support of Element 2 comprises: • **Evidence 1.1:** Letter from Head of Corporate Services supporting elements 1, 2 and 3. • **Evidence 3.1:** Information and Records Management Policy (section 5: roles and responsibilities). • **Evidence 12.1:** Information Officer's Job Description.
Action Required	No further action is required in respect of Element 2.

Element 3: Records Management Policy Statement

Element 3: Records Management Policy Statement	
Element Requirement	This is a compulsory element of the Public Records (Scotland) Act 2011. A records management policy statement underpins effective management of an authority's records and information. It demonstrates to employees and stakeholders that managing records is important to the authority and serves as a mandate for the activities of the records manager. The policy must be approved by senior management and should be made available to all staff.
Statement of Compliance	The Commissioner's office recognises the value of our records as a corporate asset providing evidence of the actions and decision making that underpin our daily functions and operations helping us to promote and safeguard the rights of children and young people in Scotland; and that their management is a key corporate function. Our commitment and overall approach to records management is set out in our Information and Records Management Policy. This policy applies to the Commissioner and every member of staff employed by the Commissioner. No function of the Commissioner (as defined under the Commissioner for Children and Young People (Scotland) Act 2003) is contracted out to a third party.
Evidence of Compliance	Evidence submitted in support of Element 3 comprises: • **Evidence 1.1:** Letter from Head of Corporate Services supporting elements 1, 2 and 3. • **Evidence 3.1:** Information and Records Management Policy.
Action Required	No further action is required in respect of Element 3.

Element 4: Business Classification

Element 4: Business Classification	
Element Requirement	A business classification scheme describes what business activities the authority undertakes – whether alone or in partnership. It is expected that an authority's records management plan confirms that the authority has developed or is in the process of developing a business classification scheme.
Statement of Compliance	The Commissioner's office maintains a business classification scheme which provides a structure for classifying all records regardless of format across the organisation. The scheme also provides a framework for developing and implementing a schedule for the retention and disposal of all records within the office. The scheme is primarily function based; however it does incorporate some elements of an organisational and subject based scheme, enabling staff to browse for records via broad categories.
Evidence of Compliance	Evidence submitted in support of Element 4 comprises: • **Evidence 4.1:** Business Classification Scheme.
Action Required	**RMP 4.1:** Review and update business classification scheme (BCS) in accordance with completion of retention schedule. Revised BCS to be forwarded to the Keeper as part of evidence submission. *Action to be completed November 2015.*

Element 5: Retention Schedules

Element 5: Retention Schedules	
Element Requirement	A retention schedule is a list of records for which pre-determined disposal dates have been established. An authority's records management plan must confirm that the authority has developed, or is in the process of developing, record retention and disposal schedules.
Statement of Compliance	The Commissioner's office is in the process of developing a schedule for the retention and disposal of documents and records. For records series that are complete (finance and investigation) the schedule is maintained and applied in the appraisal and disposal of records. Retention periods are determined by statutory and business requirements.
Evidence of Compliance	Evidence submitted in support of Element 5 comprises: • **Evidence 3.1:** Information and Records Management Policy (section 2: appraisal and disposal policy). • **Evidence 4.1:** Business Classification Scheme. • **Evidence 5.1:** Retention Schedule.
Action Required	**RMP 5.1:** Complete the development of a retention schedule to enable all records to be identified for review. Full retention schedule to be forwarded to the Keeper as part of evidence submission. *Action to be completed June – October 2015.* **RMP 5.2:** Update the Keeper on progress made in completing a retention schedule for all record types and its application in the appraisal and disposal of records. *Action to be completed September – December 2015.*

Element 6: Destruction Arrangements

Element 6: Destruction Arrangements	
Element Requirement	This is a compulsory element of the Public Records (Scotland) Act 2011. It is not always cost-effective or practical for an authority to securely destroy records in-house. Many authorities engage a contractor to destroy records and ensure the process is supervised and documented. It is vital that a records management plan confirms that the authority has developed or is in the process of developing proper destruction arrangements.
Statement of Compliance	Electronic documents and records are managed within the Commissioner's office via HP TRIM (an electronic document and records management system) and a Filemaker Database (Enquiries Records). HP TRIM contains an archiving component to enable the orderly disposal and destruction of records. This component is routinely applied to records managed via the current retention schedule. The Filemaker database contains an archiving component to enable the orderly disposal and destruction of records. HP TRIM is also used to identify when physical records are due for disposal and destruction. A contract is in place with Changeworks Recycling for the secure data destruction of all our physical documents and records. Changeworks is accredited and audited annually by UKSSA (UK Security Shredding Association) to their code of practice (incorporating BS EN 15713:2009). A contract is in place with Dunedin IT to manage the Commissioner's backup process. This is undertaken via a backup and recovery software solution, Storage Craft Product Suite. This solution enables onsite and offsite backups to automatically run and be deleted in line with the Commissioner's retention cycle for backups. This means that after a digital record has been deleted from its host

Element 6: Destruction Arrangements	
	system (e.g. HP Trim or Filemaker) it will continue to exist for 8 weeks in a backup file offsite. A contract is in place with Dunedin IT for the secure destruction of our IT equipment. Dunedin IT contracts this service with a third party company, Pure IT Recycling, on behalf of the Commissioner's office. Taking into account the Commissioner's responsibilities under the Data Protection Act 1998 Pure IT Recycling provide a guaranteed and certified data destruction service, by either wiping or physically destroying the items containing such data, ensuring security from the time of collection through to destruction and issuing a certificate after destruction.
Evidence of compliance	Evidence submitted in support of Element 6 comprises: • **Evidence 3.1:** Information and Records Management Policy (section 2: appraisal and disposal policy). • **Evidence 6.1:** UKSSA Certificate of Compliance of Confidential Waste Contractor. • **Evidence 6.2:** UKSSA Code of Practice. • **Evidence 6.3:** Certificate of Destruction (Example). • **Evidence 6.4:** IT Recycling & Data Destruction Services 2015-2016. • **Evidence 6.5:** IT Data Destruction Certificate (Sample). • **Evidence 6.6:** IT Support Contract (section on data destruction).
Action Required	**RMP 6.1:** Develop and apply records review procedures regardless of location and format. *Action to be completed November – January 2016.* **RMP 5.1:** Complete the development of a retention schedule to enable records to be identified for review. Full retention schedule to be forwarded to the Keeper as part of evidence submission. *Action to be completed June – October 2015.*

Element 7: Archiving and Transfer Arrangements

Element 7: Archiving and Transfer Arrangements	
Element Requirement	This is a compulsory element of the Public Records (Scotland) Act 2011. This is the mechanism by which an authority transfers records of enduring value to an appropriate archive repository, specifying the timing of transfers and other terms and conditions.
Statement of Compliance	The process for the appraisal and disposal of records within the Commissioner's office is outlined in the Information and Records Management Policy. There is a Memorandum of Understanding (MoU) between the Keeper of the Records of Scotland and the Commissioner. The MoU sets out how the process of depositing, storing and accessing records of enduring historical, cultural and research value transferred from the Commissioner to the National Records of Scotland (NRS) will operate.
Evidence of Compliance	Evidence submitted in support of Element 7 comprises: • **Evidence 3.1:** Information and Records Management Policy (section 2: appraisal and disposal policy). • **Evidence 7.1:** Memorandum of Understanding between the Keeper and the Commissioner.

Action Required	**RMP 7.1:** In consultation with the NRS agree and establish processes for the transfer of records for permanent preservation to the Government Records Branch. *Action to be completed January – March 2016.* **RMP 7.2:** The majority of records identified for permanent preservation are likely to be 'born digital' records. In consultation with NRS agree processes to fulfill the requirements of the NRS deposit agreement for electronic records. *Action to be completed January – March 2016.* **RMP 7.3:** Complete development of a retention schedule (see RMP 5.1), identifying records for permanent preservation and transfer to the NRS in the future. Completed schedule to be sent to NRS Government Records Branch for appraisal. *Action to be completed October 2015.*

Element 8: Information Security

Element 8: Information Security	
Element Requirement	This is a compulsory element of the Public Records (Scotland) Act 2011. Information security is the process by which an authority protects its records and ensures they remain available. It is the means by which an authority guards against unauthorised access and provides for the integrity of the records. Robust information security measures are an acknowledgement that records represent a risk as well as an asset. A public authority should have procedures in place to assess and contain that risk.
Statement of Compliance	The Commissioner's office recognises the importance of protecting its information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. Our approach to this is set out in our information security policy. All staff are expected to apply and adhere to this policy and in doing so ensure business continuity and minimise the occurrence and impact of information security incidents. To ensure the security of the Commissioner's records: 1. Procedures are in place to ensure the physical security of paper records; confidential information is held in a locked cabinet; 2. electronic records held on TRIM and Filemaker (electronic records management systems) have specific access rights; 3. passwords are required to access the Commissioner's network, these are changed regularly; 4. the remote working policy, and sections of the employee handbook, describe what is expected of staff in terms of information security when working out of the office; and 5. training is provided to all staff regarding data protection requirements.

Element 8: Information Security	
Evidence of Compliance	Evidence submitted in support of Element 8 comprises: • **Evidence 3.1:** Information and Records Management Policy (section 3: information security policy). • **Evidence 8.1:** Remote Working Policy. • **Evidence 8.2:** Employee Handbook (home working arrangements). • **Evidence 8.3:** HP TRIM Documentation regarding security administration. • **Evidence 9.1:** Data Protection Policy • **Evidence 9.3:** Employee Handbook (confidentiality and data protection).
Action Required	**RMP 10.1:** Consider the option of server virtualisation during 2015-16 to enhance our disaster recovery strategy and ensure greater information security of our electronic records. Ensure the Keeper is informed of any decision taken regarding this. *Action to be completed June – March 2016.*

Element 9: Data Protection

Element 9: Data Protection	
Element Requirement	An authority handling personal information about individuals has a number of legal obligations to protect that information under the Data Protection Act 1998. It is expected that an authority's Records Management Plan will indicate compliance with data protection obligations.
Statement of Compliance	The Commissioner's office has a Data Protection Policy which sets out how we comply with our obligations under the Data Protection Act. Training is provided to all staff on Data Protection Act compliance during induction, and thereafter as part of annual training. A privacy notice is published on our website informing people of what to expect when the Commissioner's office collects their personal information. The Commissioner's office is a registered data controller with the Information Commissioner's Office (ICO).
Evidence of Compliance	Evidence submitted in support of Element 9 comprises: • **Evidence 9.1:** Data Protection Policy. • **Evidence 9.2:** Certificate of Registration as a Data Controller with the Information Commissioner's Office. • **Evidence 9.3:** Employee Handbook (confidentiality and data protection). • **Evidence 9.4:** Privacy Notice.
Action Required	**RMP 9.1:** Develop procedures to compliment the data protection policy; in particular, provide guidance on responding to subject access requests and handling data protection breaches. Guidance to be forwarded to the Keeper as part of evidence submission. *Action to be completed June – September 2015.*

Element 10: Business Continuity and Vital Records

Element 10: Business Continuity and Vital Records	
Element Requirement	A business continuity and vital records plan serves as the main resource for the preparation for, responses to, and recovery from, an emergency that might affect any number of crucial functions in an authority. It is recommended that public authorities have a business continuity plan and that they can identify key records that facilitate the operation of the authority.
Statement of Compliance	The Commissioner's office has a business continuity plan, which currently acts as the sole vital record the Commissioner's office needs to recover operations. Copies of this plan are held off-site. The plan contains a section on vital records that details: the types of records considered vital; how these are to be identified; how they will be protected and retrieved in the event of a disaster. The Commissioner's annual IT support contract includes a disaster recovery service in conjunction with third parties. In the event that we should suffer a critical server failure or a loss of access to our office for an extended period, systems are in place to enable our IT support company to provide us with the necessary hardware and software to enable operations to be re-established within 2-3 days.
Evidence of Compliance	Evidence submitted in support of Element 10 comprises: • **Evidence 10.1:** Business Continuity Plan (Critical Function 1-4 and section on vital records).

Element 10: Business Continuity and Vital Records	
Action Required	**RMP 10.1:** Consider the option of server virtualisation during 2015-16 to enhance our disaster recovery strategy and ensure greater information security of our electronic records. Ensure the Keeper is informed of any decision taken regarding this. *Action to be completed June – March 2016.* **RMP 10.2:** Identify and prepare a list of vital records to be added as a record series in the retention schedule. Ensure the Keeper is informed once this action is complete. *Action to be completed August - September 2015.*

Element 11: Audit Trail

Element 11: Audit Trail	
Element Requirement	An audit trail is a sequence of steps documenting the movement and/or editing of a record resulting from activities by individuals, systems or other entities. The Keeper wishes to see reference under Records Management Plans to audit provisions in place or being developed to manage record movement and version control.
Statement of Compliance	The principal electronic document and records management system, HP TRIM, protects information from unauthorised access and provides protection of system function so users can only perform tasks necessary for their day-to-day work. HP TRIM also provides audit trails of authorised access as well as version control. It is the responsibility of all staff to manage records via the HP TRIM system. There are a number of exceptions where records are not managed via HP TRIM: enquiries records; finance records and personnel records. A Filemaker database is used to manage enquiries records. This database has restricted access. It does not however, provide audit trail functionality commensurate with its function as a repository of individual casework. Sage 50 accounts software is used to manage our finance records. Sage provides functionality to audit events such as the update of critical fields. Personnel records are retained in hard copy format. These records are managed by the Head of Corporate Services. Access to personnel records is limited to the Head of Corporate Services and the Commissioner.

Element 11: Audit Trail	
Evidence of Compliance	Evidence submitted in support of Element 11 comprises: • **Evidence 11.1:** HP TRIM Documentation regarding Audit Trail. • **Evidence 11.2:** HP TRIM Documentation regarding electronic document revisions.
Action Required	**RMP 11.1:** Improve the current information system for managing enquiries (including audit trail functionality) to take account of the changes to the Commissioner's provision of investigation under the Children and Young People (Scotland) Act 2014. Update the Keeper on progress made. *Action to be completed June – March 2016.* **RMP 11.2:** Identify and implement a process to improve the audit trail in relation to personnel records. *Action to be completed September – November 2015.*

Element 12: Competency Framework for Records Management Staff

Element 12: Competency Framework for Records Management Staff	
Element Requirement	A competency framework lists the core competencies and the key knowledge and skills required by a records manager. It can be used as a basis for developing job specifications, identifying training needs, and assessing performance.
Statement of Compliance	The Commissioner is supported in their role by a small team of 16 FTE staff located in a single office. Accordingly, a dedicated records management post is not proportionate to the size of the authority. Strategic accountability for records management forms part of the Head of Corporate Services responsibilities. They are supported in the day-to-day operation of records management by the Information Officer. The Information Officer's job description specifies their records management responsibilities. The Commissioner's office provides appropriate opportunities for training and development to support the Information Officer in fulfilling their records management responsibilities; including organisational membership of the Information and Records Management Society (IRMS).
Evidence of Compliance	Evidence submitted in support of Element 12 comprises: • **Evidence 12.1:** Information Officer's Job Description. • **Evidence 12.2:** Membership of Information and Records Management Society.

Action Required	**RMP 12.1:** Provide training to the administration officer to enable them to support the Information Officer with specific records management duties. Inform the Keeper when this is in place, and provide a sample of training materials as part of the evidence submission. *Action to be completed June – March 2016.* **RMP 12.2:** Consider external training opportunities for other members of staff in information and records management. *Action to be completed June – March 2016.*

Element 13: Assessment and Review

Element 13: Assessment and Review	
Element Requirement	Regular self-assessment and review of records management systems will give an authority a clear statement of the extent that its records management practices conform to the Records Management Plan as submitted and agreed by the Keeper.
Statement of Compliance	The Records Management Plan will be reviewed on a six monthly cycle for the first two years to ensure that where an action is required under each of the fourteen elements it is undertaken. The Governance arrangements of the Commissioner's office as outlined in the Information and Records Management policy will provide for an annual report on information and records management to the management team. The current operational plan 2015/16 incorporates a range of information management activities.
Evidence of Compliance	Evidence submitted in support of Element 13 comprises: • **Evidence 3.1:** Information and Records Management Policy (section 6: compliance and review). • **Evidence 13.1:** Operational Plan 2015-16.
Action Required	**RMP 13.1:** Undertake a six monthly review of the actions required in the Records Management Plan. *Action to be completed January 2016.* **RMP 13.2:** A records management improvement plan will be implemented by the Information Officer and Head of Corporate Services. Progress assessed monthly. *Action to be completed September 2015.* **RMP 13.3:** Self assessment of records management using the Archives and Records Management Services (ARMS) framework. *Action to be completed August 2016.*

Element 14: Shared Information

Element 14: Shared Information	
Element Requirement	Under certain conditions, information given in confidence may be shared. Most commonly this relates to personal information, but it can also happen with confidential corporate records.
Statement of Compliance	We comply with the requirements of the Data Protection Act, 1998. We do not currently undertake data sharing exercises with other organisations. We have a statutory duty to respond to requests for information made under the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004. As part of our compliance with these statutory obligations we share information openly through our publication scheme. In accordance with the Children and Young People (Scotland) Act 2014 the Commissioner became a corporate parent from April 2015. As part of our duties as a corporate parent we may be required to collaborate with other corporate parents when exercising our responsibilities (this may include information sharing). An information sharing code of practice will be developed to take account of our new duties.
Evidence of Compliance	Evidence submitted in support of Element 14 comprises: • **Evidence 9.1:** Data Protection Policy. • **Evidence 14.1:** Guide to information available through our publication scheme.
Action Required	**RMP 14.1:** Develop an information sharing code of practice and forward to the Keeper as part of evidence submission. *Action to be completed November – December 2015.*

Appendix 1 – List of Actions Required

Element		Action Required	Timescale
4	**Business Classification**	**RMP 4.1:** Review and update business classification scheme (BCS) in accordance with completion of retention schedule. Revised BCS to be forwarded to the Keeper as part of evidence submission.	November 2015
5	**Retention Schedules**	**RMP 5.1:** Complete the development of a retention schedule to enable records to be identified for review. Full retention schedule to be forwarded to the Keeper as part of evidence submission.	June – October 2015
		RMP 5.2: Update the Keeper on progress made in completing a retention schedule for all record types and its application in the appraisal and disposal of records.	September – December 2015
6	**Destruction Arrangements**	**RMP 6.1:** Develop and apply records review procedures regardless of location and format.	November – January 2016
7	**Archiving and Transfer Arrangements**	**RMP 7.1:** In consultation with the NRS agree and establish processes for the transfer of records for permanent preservation to the Government Records Branch.	January – March 2016
		RMP 7.2: The majority of records identified for permanent preservation are likely to be 'born digital' records. In consultation with NRS agree processes to fulfil the requirements of the NRS deposit agreement for electronic records.	January – March 2016
		RMP 7.3: Complete development of a retention schedule (see RMP 5.1),	October 2015

Element		Action Required	Timescale
		identifying records for permanent preservation and transfer to the NRS in the future. Completed schedule to be sent to NRS Government Records Branch for appraisal.	
9	**Data Protection**	**RMP 9.1:** Develop procedures to compliment the data protection policy; in particular provide guidance on responding to subject access requests and handling data protection breaches. Guidance to be forwarded to the Keeper as part of evidence submission.	June – September 2015
10	**Business Continuity and Vital Records**	**RMP 10.1:** Consider the option of server virtualisation during 2015-16 to enhance our disaster recovery strategy and ensure greater information security of our electronic records. Ensure the Keeper is informed of any decision taken regarding this.	June – March 2016
		RMP 10.2: Identify and prepare a list of vital records to be added as a record series in the retention schedule. Ensure the Keeper is informed once this action is complete.	August - September 2015
11	**Audit Trail**	**RMP 11.1:** Improve the current information system for managing enquiries (including audit trail functionality) to take account of the changes to the Commissioner's provision of investigation under the Children and Young People (Scotland) Act 2014.	June – March 2016
		RMP 11.2: Identify and implement a process to improve the audit trail in relation to personnel records.	September – November 2015

Element		Action Required	Timescale
12	**Competency Framework for Records Management Staff**	**RMP 12.1:** Provide training to the administrative officer to enable them to support the Information Officer with specific records management duties. Inform the Keeper when this is in place, and provide a sample of training materials as part of the evidence submission.	June – March 2016
		RMP 12.2: Consider external training opportunities for other members of staff in information and records management.	June – March 2016
13	**Assessment and Review**	**RMP 13.1:** Undertake a six monthly review of the actions required in the Records Management Plan.	January 2016
		RMP 13.2: A records management improvement plan will be implemented by the Information Officer and Head of Corporate Services. Progress assessed monthly.	September 2015
		RMP 13.3: Self assessment of records management using the Archives and Records Management Services (ARMS) framework.	August 2016
14	**Shared Information**	**RMP 14.1:** Develop an information sharing code of practice and forward to Keeper as part of evidence submission.	November – December 2015

Appendix 2 – Schedule of Evidence

Element		Evidence
1	**Senior Management Responsibility**	**Evidence 1.1:** Letter from Head of Corporate Services supporting elements 1, 2 and 3.
		Evidence 3.1: Information and Records Management Policy (section 5: roles and responsibilities).
2	**Records Manager Responsibility**	**Evidence 1.1:** Letter from Head of Corporate Services supporting elements 1, 2 and 3.
		Evidence 3.1: Information and Records Management Policy (section 5: roles and responsibilities).
		Evidence 12.1: Information Officer's Job Description.
3	**Records Management Policy Statement**	**Evidence 1.1:** Letter from Head of Corporate Services supporting elements 1, 2 and 3.
		Evidence 3.1: Information and Records Management Policy.
4	**Business Classification**	**Evidence 4.1:** Business Classification Scheme.
5	**Retention Schedules**	**Evidence 3.1:** Information and Records Management Policy (section 2: appraisal and disposal policy).
		Evidence 4.1: Business Classification Scheme.
		Evidence 5.1: Retention Schedule.
6	**Destruction Arrangements**	**Evidence 3.1:** Information and Records Management Policy (section 2: appraisal and disposal policy).

Element		Evidence
		Evidence 6.1: UKSSA Certificate of Compliance of Confidential Waste Contractor.
		Evidence 6.2: UKSSA Code of Practice.
		Evidence 6.3: Certificate of Destruction (Example).
		Evidence 6.4: IT Equipment Disposal and Recycling Process.
		Evidence 6.5: IT Data Destruction Certificate (Sample).
7	**Archiving and Transfer Arrangements**	**Evidence 3.1:** Information and Records Management Policy (section 2: appraisal and disposal policy).
		Evidence 7.1: Memorandum of Understanding between the Keeper and the Commissioner.
8	**Information Security**	**Evidence 3.1:** Information and Records Management Policy (section 3: information security policy).
		Evidence 8.1: Remote Working Policy.
		Evidence 8.2: Employee Handbook (home working arrangements).
		Evidence 8.3: HP TRIM Documentation regarding security administration.
		Evidence 9.1: Data Protection Policy.
		Evidence 9.3: Employee Handbook (confidentiality and data protection).
9	**Data Protection**	**Evidence 9.1:** Data Protection Policy.

Element		Evidence
		Evidence 9.2: Certificate of Registration as a Data Controller with the Information Commissioner's Office.
		Evidence 9.3: Employee Handbook (confidentiality and data protection).
		Evidence 9.4: Privacy Notice.
10	**Business Continuity and Vital Records**	**Evidence 10.1:** Business Continuity Plan (section on vital records).
11	**Audit Trail**	**Evidence 11.1:** HP TRIM Documentation regarding Audit Trail.
		Evidence 11.2: HP TRIM Documentation regarding electronic document revisions.
12	**Competency Framework for Records Management Staff**	**Evidence 12.1:** Information Officer's Job Description.
		Evidence 12.2: Membership of Information and Records Management Society.
13	**Assessment and Review**	**Evidence 3.1:** Information and Records Management Policy (section 6: compliance and review).
		Evidence 13.1: Operational Plan 2015-16.
14	**Shared Information**	**Evidence 9.1:** Data Protection Policy.
		Evidence 14.1: Guide to information available through our publication scheme.

Appendix 3 – Evidence (Extracts and Documents)

Evidence 1.1: Letter from Head of Corporate Services supporting elements 1, 2 and 3.

27 April 2015

The Keeper of the Records of Scotland
National Records of Scotland
General Register
House 2 Princes
Street Edinburgh
EH1 3YY

Dear Sir,

Public Records (Scotland) Act 2011
Element 1: Senior Management Responsibility
Element 2: Records Manager Responsibility
Element 3: Records Management Policy
Statement

Under the Public Records (Scotland) Act 2011, Scotland's Commissioner for Children and Young People must prepare a Records Management Plan (RMP) and ensure that their public records are managed in accordance with the RMP.

I write to inform you that as Head of Corporate Services and a member of the Commissioner's Management Team, I have overall strategic responsibility for records management within the Commissioner's office *(Element 1)*. The Commissioner's RMP, submitted for agreement to you, has been approved and receives the support of the Management Team. Gillian Munro, Information Officer, has overall day-to-day responsibility for the implementation of the RMP within the Commissioner's office *(Element 2)*.

A records management policy has been prepared as part of the RMP which I have endorsed *(Element 3).* This policy is made available to all staff and each member of the Management Team is responsible for the dissemination and implementation of it within their team.

Yours faithfully,

Stephen Grounds,
Head of Corporate Services

Information and Records Management Policy

April 2015

Contents

1 Records Management Policy

1.1 Policy Statement

Our records are our corporate memory providing evidence of the actions and decision making that underpin our daily functions and operations and help us to promote and safeguard the rights of children and young people in Scotland. This policy and its related procedures and guidance have been produced to help us ensure that adequate records are held by the Commissioner's office and that they are managed and controlled effectively, and in support of our legal, operational and information needs.

1.2 Scope

The Commissioner and every member of staff employed by the Commissioner must comply with this records management policy and related policies, procedures and guidelines.

In records management it is important to be clear about the difference between a document and a record. A document is any piece of information produced or received by an organisation or a person. Some documents will be of temporary value and need never end up in a records management system (such as an invitation to lunch). Some documents will need to be kept as evidence of operational transactions, routine activities, or as a result of legal obligations. These should be placed into an official filing system and at this point they become records.

This policy covers all records held by the Commissioner's office regardless of format. This policy therefore covers records in the following formats:

- Audio and video tapes, cassettes, DVD film, podcasts
- Email (including work information held in personal email accounts)
- Facsimile (Fax)
- Photographs
- Records in all electronic formats, including disks or CDs
- Records in paper format

This policy also covers all records in the above formats that have been transferred to the Commissioner's office by external organisations and individuals, for the duration of the time that they remain in the care of the Commissioner's office.

1.3 Policy Objectives

The Public Records (Scotland) Act 2011 places an obligation on named authorities, including the Commissioner, to produce a records management plan which sets out their arrangements for the effective management of all records.

This policy and associated procedures and guidelines are intended to ensure that all records held by the Commissioner's office are effectively managed throughout their lifecycle, from planning and creation through to disposal. There are eight key elements to this policy:

1.3.1 Support

Records Management is recognised as a core corporate function with defined roles and lines of responsibility. The Commissioner and their staff are made aware of the benefits of good records management and understand their own record-keeping responsibilities through generic and specific training programmes and guidance.

1.3.2 Accountability and Compliance

Complete and accurate records are kept for operational, regulatory, legal and accountability purposes. In particular the records kept must take into account the following:

- The legislative and regulatory environment within which the Commissioner's office operates
- The need to facilitate audit or examination
- The need to provide credible and authoritative evidence
- The need to protect legal and other rights of the Commissioner, their office, staff and its stakeholders; and
- The need to allow public access to authoritative information about the functions provided by the Commissioner and their office; the cost of providing those functions; the standard attained in fulfilling those functions; the evidence which forms the basis of decisions and actions taken by the Commissioner and their office; and the publication of reasons for decisions taken.

1.3.3 Quality

Records are authentic, complete and accurate. Their contents should be reliable and their integrity guaranteed.

1.3.4 Accessibility and Usability

Records and the information within them can be easily stored, located, retrieved and used by those with a right of access, for as long as necessary.

1.3.5 Compliance

Records comply with any record keeping requirements resulting from the legislative and regulatory environment. Particular regard must be paid to our duties as a data controller as defined in the Data Protection Act 1998 and the section 61 code of practice on records management

1.3.6 Security

Records will be secure from unauthorised or inadvertent alteration or deletion, whilst access to and disclosure of them will be properly controlled. Particular care should be taken with personal information about living individuals to ensure compliance with the Data Protection Act.

1.3.7 Review and Disposal

There are documented retention, selection and disposal schedules to define how long particular records should be kept, disposed of and explain why records are no longer held.

1.3.8 Monitoring

The application of records management procedures are regularly monitored and reviewed; and action taken to improve standards as and when required. An annual report on information and records management will be submitted to the Management Team.

1.4 Records Management

1.4.1 Record Creation

It is the responsibility of all staff to ensure that all official documents that record essential activities are filed in an appropriate manner. These records should be complete and accurate enough to enable current staff and their successors to fulfil their responsibilities to:

- facilitate an audit of examination of the Commissioner's office by anyone so authorised;
- protect the legal and other rights of the Commissioner's office, its clients and any other persons affected by its actions;
- provide proof of the authenticity of the records so that the evidence derived from them is shown to be credible and authoritative; and

- provide a true and accurate record of the principal policies and activities of the Commissioner's office of ongoing public accountability and interest.

Records are primarily managed within the Commissioner's office via electronic records and document management systems. These systems: accommodate paper and electronic records; provide simple information architecture for file storage; and provide referencing and classification metadata for the registration of records with quick and easy retrieval of accurate information. It is the responsibility of all staff to save records to the appropriate records management system. Emails generated or received by staff are subject to the same records management principles as the equivalent information in any other format.

Whilst the majority of records are managed within an electronic records and document management system there are a number of exceptions:

- evidence provided by external parties in the course of an investigation;
- records received in paper format that are of sufficient bulk they are impractical to scan;
- printed copies of electronic records for reference purposes; and
- printed publications that form part of an on-site archive.

1.4.2 Record Indexing

Our records must be trustworthy, complete, accessible, legally admissible in court, and robust for as long as our records retention schedule requires. Records that are consistently and logically indexed are easier to manage to meet these requirements. Staff should therefore reference, title, index and security mark records they create and/or receive from external sources with the appropriate metadata. The metadata added should be easily understood by all staff and enable the efficient retrieval of information.

1.4.3 Record Maintenance

The design and configuration of information architecture within any records management system will ensure that records and the information they contain can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held. Staff should regard our current records collection as a knowledge bank of experience and expertise. The information held in our records can and should be used as a key resource to inform our current and future work.

A key factor in ensuring that our decision making processes and the actions that we take are of a high standard is the ability to access the most up-to-date

information available. It is therefore vital that all staff adhere to version control procedures, when amending and updating records. The design and configuration of information architecture within any of our records management systems will ensure that there is an auditable trail of record transactions.

All staff must follow the information security policy (see Section 3) to ensure that all records are secure from unauthorised or inadvertent alteration or erasure and that access and disclosure of records and the information they contain is properly controlled. The information security policy outlines a formal process for removal of records; this also covers copies of records removed by contractors (as a legitimate requirement of the work they are undertaking on our behalf) or other relevant parties (e.g. Police Scotland as part of an investigation).

Official records in paper format should be managed in a filing system that is consistent with the corporate classification scheme. Each record should have a matching metadata record in the electronic records management system. Metadata should include location details.

1.4.4 Records Retention and Disposal

A retention schedule is under development to support the control of records by determining the record types for creation, storage and final disposition to meet our operational needs and ensure our compliance with legal requirements. The Commissioner's office has a retention schedule for managing finance and investigation records; the schedule is under development to help manage all records. The retention schedule is an essential component of efficient and effective records management and where available must be consistently implemented by all staff. The records appraisal and disposal policy (see Section 2) sets out the arrangement for managing and recording the final disposition decisions for all our records when they come to the end of their useful life.

1.4.5 Compliance, Governance and Risk

The electronic document and records management systems used log all records activity. This provides an audit trail which can be used as part of system monitoring and compliance auditing. The management and auditing of all information held in our electronic document and records management systems complies with the code of practice for Evidential Weight and Legal Admissibility of Electronic Information, BS 10008:2008; see section 4 for further information.

The Commissioner's office has a business continuity plan which documents the processes to be undertaken in the event of a disruption to service affecting the

normal business activities. The plan includes a maintenance and preservation policy which sets out the procedures that must be followed to protect our official records in the event that any of the listed disaster scenarios should occur. The business continuity plan is complemented by a risk register which lists records management as a standing item.

2 Appraisal and Disposal Policy

2.1 Policy Statement

This policy sets out the arrangement for managing appraisal and recording the final disposal decision for records when they cease to be active and come to the end of their useful life. The Data Protection Act, Freedom of Information (Scotland) Act and the Environmental Information (Scotland) Regulations impose stringent duties on public authorities to prevent the ad hoc disposal of records and ensure that final disposal decisions are based on a pre-defined criteria and clearly articulated processes.

2.2 Policy Objectives

This policy will support the Commissioner's office to manage and control its records effectively by providing appropriate guidance for authoritative and auditable disposal decisions and actions. Specifically this policy and associated procedures will:

- assist in identifying records that may be worth preserving permanently as part of the archives of the Commissioner's office;
- prevent the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration;
- provide consistency for the destruction of those records not required permanently after specified periods; and
- avoid the costs and liabilities of retaining information no longer required by the office that may lead to non-compliance with legislation (DPA, FOISA, and EIRs) and possible legal action against the Commissioner.

2.3 Records Retention Schedule

The purpose of the retention schedule is to support the appraisal and disposal policy by determining the record types for creation, storage and final disposal. The Commissioner's office will continue to develop a schedule for the retention and disposal of records. The preparation and maintenance of this will primarily be the responsibility of the Information Officer with input from colleagues to reflect the activities and functions of the office. The retention schedule will outline how long each category of record held by the Commissioner's office should be retained for and how it should be disposed of. The decisions made for retention and disposal

will be based on a number of criteria: business requirements; statutory and regulatory obligations and historical value. The schedule will require review to take account of changes (for example legislative change or the removal and addition of record types). All records indexed into the various records management systems must be dated in accordance with the retention periods stipulated in the retention schedule.

2.4 Selecting Records for Appraisal

The Commissioner's office will review proposed disposals, approve or modify retentions and select records that will be retained permanently through a process of appraisal. Reports from the electronic document records management system will be used to identify records due for appraisal. Records no longer required for statutory reasons or for business requirements should be appraised under the criteria set out in the retention schedule to establish their long term future. The appraisal process must show:

- what records are designated for destruction;
- the reason for their destruction;
- by whose authority destruction has been approved;
- when they are due for destruction;
- what records are selected for permanent preservation; and
- when and if they are to be transferred to an external archive for preservation

2.5 Records Selected for Permanent Preservation

Records should be selected for permanent preservation that show the significance of the functions and activities of the Commissioner and their office in respect of:

- the history and development of the role of Commissioner, the Commissioner's office and associated achievements, policies and procedures;
- the delivery of the function, duties and powers of the Commissioner for Children and Young People (Scotland) Act 2003;
- notable events or persons where the records add significantly to what is already known; and
- demographic and social history by means of statistics and quantitative research.

Records selected for permanent preservation shall be transferred to the National Records of Scotland (NRS) Government Records Branch. The Commissioner has a

Memorandum of Understanding with the Keeper of the Records of Scotland on how the process of depositing, storing and accessing records of enduring historical, cultural and research value transferred to the NRS will operate.

2.6 Records Selected for Destruction

Records selected for destruction should be destroyed within the timeframe cited in the retention schedule and follow procedures for the secure destruction of those records. It is important that records are kept for as long as their contents have operational value and for as long as they may be required as evidence of the transactions they document. However, there are often compelling reasons not to retain such records for any longer than they are required relating to: costs of storage, pressure on physical space; needing to disclose all relevant information held in response to a freedom of information request; and legal obligations under the DPA to not retain personal data for longer than is necessary.

2.6.1 Destruction of physical records

The Commissioner's office holds a very small number of physical records. Physical records that contain sensitive personal data, financial data or are protectively marked papers must be placed in confidential waste bags which are kept in a lockable cupboard. These bags will be collected by our third party contractor responsible for the secure destruction of our confidential waste. The third party contractor will issue a certificate of destruction with the number of confidential waste bags collected and destroyed on a particular date. Physical records awaiting destruction which contain sensitive personal data must be kept in a lockable cupboard within the Commissioner's office. All other physical records ready for destruction should be placed in recycling bags.

2.6.2 Destruction of digital records and data

The majority of records held by the Commissioner's office are born 'digital records'. As indicated in section 2.4 reports from the electronic document records management system will be used to identify records due for destruction. The destruction of digital records is different to the destruction of physical records. It is important to remember that deletion from a server may not be sufficient as although the record may no longer be visible it is not yet beyond the possibility of recovery as it will be available via a backup file (see section 2.6.3 below). Where copies of digital records are also held these must be identified and destroyed, otherwise they will still be considered to be held for the purposes of freedom of information and subject access requests.

2.6.3 Destruction of back-ups

All digital records are stored on one of three in-house servers. Our IT support company, Dunedin IT, are contracted to manage the backup of all three servers in-house and offsite. Dunedin IT use a backup and disaster recovery software solution, Storage Craft Product Suite, to automatically manage the backup process. This software enables a continual incremental backup schedule to be set up by Dunedin IT and automatically maintained. Backup image files are collapsed into daily, weekly and monthly files. Our retention of backup files is as follows:

- 4 x daily (calendar days) backups of each server
- 15 calendar days of backups
- 1 x weekly backup
- 2 x months of weekly backups
- 1 x monthly backup

As part of this process backup files are automatically deleted onsite and offsite in line with this retention cycle. In accordance with this cycle a digital record will exist in a backup store for 8 weeks after it has been selected for destruction. Dunedin IT use 'Pulsant' as their chosen partner to provide a secure offsite backup data centre. The Commissioner's backup data is stored in purpose built Tier 3 data centre facilities at South Gyle and Newbridge. All of Pulsant's services are certified and audited every six months to meet a wide range of industry standards, including ISO 27001.

Onsite backups are stored on Network Attached Storage (NAS) devices held within a locked server room within the Commissioner's office. When an onsite NAS device needs to be replaced it must be destroyed as per the Commissioner's contract with Dunedin IT for data destruction, and a certificate of destruction provided. This certificate will be retained and kept alongside the fixed asset register.

2.7 Records Destruction Register

A record of the destruction of records, showing their reference, description, reason for destruction, on whose authority they have been destroyed and date of destruction should be maintained in line with the FOISA section 61code of practice on records management.

3 Information Security Policy

3.1 Policy Statement

The purpose of this policy is to establish a framework to protect information and information systems within the Commissioner's office from unauthorised access, use, disclosure, disruption, modification or destruction; whether internal or external, deliberate or accidental. The policy correctly applied and adhered to will achieve a comprehensive and consistent approach throughout the office, ensure business continuity, and minimise the occurrence and impact of information security incidents and breaches.

3.2 Scope

The Commissioner and all staff employed by the Commissioner must comply with this information security policy and related policies, procedures and guidelines. This policy covers all information held by the Commissioner's office regardless of the format it is held in.

3.3 Management of Information Security

At corporate level, responsibility for information security shall reside with the Head of Corporate Services. All information security events and suspected weaknesses should be reported to the Head of Corporate Services at the earliest opportunity. The Head of Corporate Services shall keep the Management team informed of the information security status of the office. In the event of loss of office equipment, staff are advised to notify both the Police and the Head of Corporate Services as soon as possible. Where the damage, loss or theft is of sensitive personal information, this must be reported immediately to the Head of Corporate Services and Information Officer to enable a data protection breach to be dealt with appropriately. All information security events shall be investigated to establish their cause and impact with a view to avoiding similar events.

3.4 Contracts of Employment

Staff security requirements are addressed at the recruitment stage and all contracts of employment contain a confidentiality clause stating that each member of staff has a contractual duty not to misuse information they acquire in the course of their work or disclose information that is received in confidence from others. This applies even after they leave the Commissioner's employment.

3.5 Access Controls

Access to information and computer facilities shall be available to all staff unless there is reason to restrict access for the purposes of business, personal security and/or confidentiality. Each staff member has a unique password for logging on to the server and an automatic prompt requires this to be changed at three-monthly intervals. Staff must take all reasonable steps to ensure that they do not unnecessarily compromise the security of the office's ICT systems.

3.6 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis. In addition the Commissioner reserves the right to monitor activity where they suspect that there has been a breach of policy. This shall be undertaken in accordance with the Regulation of Investigatory Powers Act (2000) and the Human Rights Act.

3.7 Remote working

Staff provided with office equipment to work remotely must only use this for legitimate work-related purposes. This equipment should not be removed from the office without the prior approval of the Head of Corporate Services. The equipment provided may only be modified or replaced by the Commissioner's IT Contractors if authorised by the Head of Corporate Services. Office equipment must be returned at the end of the remote working arrangement. Staff should adhere to the remote working policy taking sensible precautions to protect against the loss or interference with all work related information and equipment.

3.8 Internet Use

Utilising the vast amount of information available on the internet can be integral to the work of the office. Access to the internet demands a level of trust and responsibility. This is one of the main reasons staff are requested to only visit websites necessary to complete their work and think twice before accessing sites for personal use. In general you should not send or receive information via the internet unless you are sure that the transmission is legal and secure.

A number of web sites are also available which allow the sharing and manipulation of information, for example Dropbox, pdftoword.com, and others. All staff are urged to use caution when using these resources as they may not be sufficiently secure to ensure the integrity of our information.

3.9 Malicious Software

The Commissioner's office uses software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. All staff should take reasonable steps to ensure that no viruses are transmitted to third parties and to ensure that they do not knowingly allow a virus to affect the office network. Users shall not download or install software on office equipment or network without permission from the Head of Corporate Services.

3.10 Hard Copy Information

Hard copy confidential information (including printed copies of digital information) should be held securely in a locked cabinet; the information should not be left where unauthorised persons might have sight of them. Hard copy confidential information (e.g. records containing sensitive personal data) should only be removed from the office with the prior permission of the Commissioner or Head of Corporate Services. Where confidential information is removed staff must take all reasonable steps to ensure it remains secure at all times, and that confidentiality is maintained at a level appropriate to the content of the material.

4 Legal Admissibility Policy

4.1 Policy Statement

The majority of our official records are held electronically. There may be occasions when some of these records will be required as evidence in a court of law, whether in a criminal or civil court. This policy statement explains the measures taken by the Commissioner's office to maximize the legal admissibility and evidential weight of these records.

4.2 Electronic Records and the Issue of Legal Admissibility

Legal admissibility concerns whether or not a piece of evidence would be accepted by a court of law. To ensure admissibility information needs to be managed by a secure system throughout its lifetime. Electronic records are particularly vulnerable to tampering because it is possible to make additions or deletions that are not apparent to the viewer of the document. It can also be difficult to tell the difference between the original, authentic record and copies of it which may have been altered.

If the authenticity of an electronic record required as evidence in court cannot be proven the evidential weight placed on that record would be reduced, which has the potential to harm severely the case being fought.

4.3 Measures Taken to Maximise Legal Admissibility

This information and records management policy and related policies and procedures have been developed in line with the requirements of 'British Standard 10008:2008 Evidential Weight and Legal Admissibility of Electronic Information – Specification'. The Standard sets out the requirements for the implementation and operation of electronic information management systems, including the storage and transfer of information, and addresses issues relating to authenticity and integrity of information. Our compliance with this Standard increases the likelihood that any electronic information held and required as evidence by a court of law will be afforded the maximum evidential weight.

5 Roles and Responsibilities

5.1 The Commissioner

The Commissioner has overall responsibility for ensuring that records are managed responsibly and securely within the office, and has delegated the overall strategic accountability for records management and information security to the Head of Corporate Services.

5.2 Head of Corporate Services

The Head of Corporate Services with the support of the Information Officer has responsibility for ensuring compliance with this information and records management policy, and for reviewing and updating it as necessary. The key responsibilities of the Head of Corporate Services and Information Officer are to:

1. Ensure that the Commissioner's office complies with the Public Records (Scotland) Act 2011 and the S61 Code of Practice on Records Management.
2. Review and update this policy and associated guidelines to ensure they continue to support the records management requirements of the Commissioner's office in the undertaking of its operational and statutory functions.
3. Arrange for the annual review and disposal of files.
4. Manage the audit programme and ensure any corrective actions are carried out.
5. Report and address any breaches to or suspected weaknesses of information security.
6. Provide appropriate training, guidance and feedback mechanisms to support staff in carrying out their records management and information security responsibilities.

5.3 All Staff

It is the responsibility of all staff to ensure that they keep appropriate records of their work and manage those records in keeping with this policy and associated procedures and guidance. All staff shall comply with the information security policy and associated procedures; with each member of staff individually responsible for the security of their physical environment where information is processed or stored and for the operational security of the information systems they use.

5.4 External Contractors

Contracts with external contractors that require access to the electronic and document records management systems of the Commissioner's office shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external party shall comply with all appropriate information security policies.

5.5 Training and Support

Training and support is recognised by the Commissioner's office as essential to the successful implementation of its information and records management policy. To this end appropriate training and guidance is provided to all staff. Information and records management and information security training shall be included in the staff induction process. This shall be supported by an annual training session to remind all staff of their responsibilities and highlight any changes to policy and procedures. The Information Officer will provide ongoing guidance and support to all staff on records management and information security.

6 Compliance and Review

Compliance with this policy and related policies and guidance will be monitored by the Information Officer in consultation with the Head of Corporate Services. A report on information and records management will be made annually to the management team. The purpose of the report is to provide assurance that:

- our records are being managed in accordance with published policies and guidance;
- records are held for the appropriate time;
- records are destroyed at the appropriate time;
- information is held securely; and
- personal data is lawfully processed

Reviews of this policy will take place at least every two years to take account of any new or changed legislation, regulations or business practice.

7 Related Policies and Guidance

The information and records management policy relates to the following internal policies and procedures of the Commissioner's office:

- Data Protection Policy
- Freedom of Information Policy
- Remote Working Policy
- Business Continuity Plan

It is supported by the following related procedures and guidance documents:

- Business Classification Scheme

The current version of all of these policies and procedures are held on TRIM.

8 Relevant Legislation and Regulations

8.1 Legislation and Statutory Guidance

This policy supports compliance with the following legislation and statutory guidance:

- Public Records (Scotland) Act 2011
- Scottish Ministers' Code of Practice on Records Management by Scottish Public Authorities 2011
- Equality Act 2010
- Environmental Information (Scotland) Regulations 2004
- Freedom of Information (Scotland) Act 2002
- Electronic Communications Act 2000
- Human Rights Act 1998
- Data Protection Act 1998

8.2 International Standards

The Commissioner's office aims to operate in accordance with the following best practice standards for records management and information security.

- BS ISO 10008:2008 – Evidential Weight and Legal Admissibility of Electronic Information
- ISO/IEC 27001 – Information Security Management
- BS ISO 15489:2001 – Information and Documentation – Records Management

Appendix 1: Glossary of Terms

Appraisal	The process of determining the value of records for further use, for whatever purpose, and the length of time for which that value will continue. Also referred to as evaluation, review or selection.
Archives	Records, usually but not necessarily non-current records, of enduring value selected for permanent preservation.
Audit Trail	A record showing the transactions within an information management system providing evidence of activities, such as who has accessed a computer system and when, what operations he or she has performed during a given time and the resulting changes to records or information.
Classification Scheme	A full representation of the business of an organisation, which systematically identifies and documents the organisation's activities and resulting records according to logically structured conventions, methods and procedural rules. Sometimes also referred to as a business classification scheme or file classification system.
Destruction	The disposal of records through incineration, pulping, shredding, deletion or another method, so that it is impossible to reconstruct the records.
Disposal	The actions taken to fulfil the requirements outlined in appraisal reports and retention and disposal schedules to retain, destroy or transfer records. Note that disposal is not synonymous with destruction, though destruction may be one disposal option. Also known as disposition.
Document	Information or data fixed in some medium, which may or may not be considered in whole or in part an official record.
Electronic Document and Records Management System	An electronic system or process – managed with the aid of computers and software – implemented in order to manage both electronic documents and electronic records within an organisation.
Indexing	The process of establishing terms to describe and provide access to records and archives.
Legal Admissibility	Whether or not a piece of evidence would be accepted by a court of law.
Metadata	Defined in very general terms as 'data about data' and is necessary in order to understand the context, purpose, extent and location of a record. Examples of metadata can include information relating to a record's creator, creation date, receipt date, editor, access history and disposal.
Migration	The act of moving data or records in electronic form from one hardware or software system or configuration to another so that

	they may continue to be understandable and usable for as long as they are needed.
Record	Recorded information, regardless of medium or characteristics, created, received, and maintained by an organization or person in pursuance of legal obligations or in the transaction of business activities.
Records Management	The process whereby an organisation manages its records, whether created internally or externally and in any format or media type, from their creation or receipt, through to their destruction or permanent preservation.
Retention Schedule	Defines how long records need to be retained in order to satisfy operational, legal and regulatory purposes; helps co-ordinate their appraisal, disposal or preservation.
Version Control	The management of documents or records in order to keep track of changes and revisions and ensure the most current version remains available for use.
Vital Records	A record that is essential to the organisation's operation or to the resumption of the organisation's operations after a disaster. Also known as an essential record.

Evidence 4.1: Business Classification Scheme

Function	Activity	Sub Activity
Child Rights Monitoring	**Children's Rights Impact Assessment (CRIA)**	Assessments
Child Rights Monitoring	**UNCRC Incorporation**	Advisory Group
Child Rights Monitoring	UNCRC Incorporation	Briefings & Discussion Papers
Child Rights Monitoring	UNCRC Incorporation	Research & Information
Child Rights Monitoring	**UNCRC Reporting**	3rd Periodic Report
Child Rights Monitoring	UNCRC Reporting	4th Periodic Report
Child Rights Monitoring	**Universal Periodic Review (UPR)**	1st UPR Cycle
Child Rights Monitoring	Universal Periodic Review (UPR)	2nd UPR Cycle
Corporate Management	**Agreements**	Memorandum of Understanding
Corporate Management	**Corporate Administration**	General Administration
Corporate Management	Corporate Administration	Master Forms & Templates
Corporate Management	Corporate Administration	Policies, Procedures & Handbooks
Corporate Management	**Equality Duty**	Equality Survey
Corporate Management	Equality Duty	Equality Outcomes Consultation
Corporate Management	Equality Duty	Project Management
Corporate Management	Equality Duty	Equality Steering Group
Corporate Management	Equality Duty	Mainstreaming Report & Action Plan
Corporate Management	Equality Duty	Equality Impact Assessment
Corporate Management	**Governance**	Delegation & Decision Making
Corporate Management	Governance	Environmental Management
Corporate Management	Governance	Legal Status

Function	Activity	Sub Activity
Corporate Management	Governance	Legislation
Corporate Management	Governance	Indemnity
Corporate Management	Governance	Shared Services
Corporate Management	**Meetings**	Corporate Services
Corporate Management	Meetings	Management
Corporate Management	Meetings	Participation & Education
Corporate Management	Meetings	Policy
Corporate Management	Meetings	Staff
Corporate Management	**Quality & Performance**	
Corporate Management	**Risk Management**	Business Continuity
Corporate Management	Risk Management	Health and Safety
Corporate Management	Risk Management	Risk Assessment
Corporate Management	Risk Management	Risk Register
Corporate Management	Risk Management	Wellbeing
Corporate Management	**Strategy & Planning**	Corporate Parenting Plan
Corporate Management	Strategy & Planning	Drafting Plans
Corporate Management	Strategy & Planning	Safe, Active, Happy 2006-2009
Corporate Management	Strategy & Planning	Strategic Plan
External Communication & Relations	**Articles, Presentations and Speeches**	Sub levels arranged by year
External Communication & Relations	**BINOCC**	Sub levels arranged by meeting
External Communication & Relations	**Commissioner Correspondence**	Sub levels arranged by year
External Communication & Relations	**Commissioner Diary**	Sub levels arranged by year

Function	Activity	Sub Activity
External Communication & Relations	**Communications Administration**	Accessible Communications
External Communication & Relations	Communications Administration	Communications Strategy
External Communication & Relations	Communications Administration	Corporate Guidelines
External Communication & Relations	Communications Administration	Image Library
External Communication & Relations	Communications Administration	Illustrations
External Communication & Relations	**COSLA**	
External Communication & Relations	**Digital Media**	Website Audit
External Communication & Relations	Digital Media	Market Research
External Communication & Relations	Digital Media	Analytics
External Communication & Relations	**ENOC**	Sub levels arranged by year
External Communication & Relations	**Events and Engagement**	Administration
External Communication & Relations	Events and Engagement	Current Events
External Communication & Relations	Events and Engagement	ENOC Conference
External Communication & Relations	Events and Engagement	Past Events
External Communication & Relations	**Media Relations**	Correspondence
External Communication & Relations	Media Relations	Public Relations
External Communication & Relations	Media Relations	Media Cuttings
External Communication & Relations	Media Relations	Press Releases & Statements
External Communication & Relations	**Partnership & Collaborative Working**	Groups & Networks
External Communication & Relations	Partnership & Collaborative Working	Planning
External Communication & Relations	Partnership & Collaborative Working	Protocols & Agreements
External Communication & Relations	**Publications**	Dissemination

Function	Activity	Sub Activity
External Communication & Relations	Publications	Final
External Communication & Relations	Publications	Preparation
External Communication & Relations	**Scottish Government Relations**	Correspondence
External Communication & Relations	Scottish Government Relations	Child Rights Team
External Communication & Relations	Scottish Government Relations	Ministerial Correspondence
External Communication & Relations	Scottish Government Relations	Groups & Taskforces
External Communication & Relations	**Scottish Parliament Relations**	Scottish Parliament Information
External Communication & Relations	Scottish Parliament Relations	SPCB
External Communication & Relations	Scottish Parliament Relations	MSPs Correspondence
External Communication & Relations	**UK Government Relations**	Correspondence
Facilities Management	**Construction**	
Facilities Management	**Insurance**	
Facilities Management	**Lease**	
Facilities Management	**Maintenance and Repair**	
Finance	**Accounts Management & Audit**	Audit Advisory Board
Finance	Accounts Management & Audit	Audit Reports
Finance	**Budget**	Annual Budget
Finance	**Financial Administration**	Committee
Finance	Financial Administration	General Administration
Finance	Financial Administration	Master Form & Templates
Finance	**Payroll & Pensions**	Expenses
Finance	Payroll & Pensions	Payroll

Function	Activity	Sub Activity
Finance	Payroll & Pensions	Pensions
Finance	**Procurement**	Closed Contracts
Finance	Procurement	Current Contracts
Finance	Procurement	Payment of Invoices
Finance	Procurement	Tendering
Finance	Procurement	Unsuccessful Tenders
Human Resources	**Administration**	
Human Resources	**Commissioner**	Appointment
Human Resources	**Disclosure**	
Human Resources	**Equal Opportunities**	Policies & Procedures
Human Resources	Equal Opportunities	Monitoring & Analysis
Human Resources	**Performance Management**	Appraisal
Human Resources	**Personnel Files**	
Human Resources	**Recruitment**	Applications
Human Resources	Recruitment	Campaigns / Adverts
Human Resources	Recruitment	Correspondence
Human Resources	Recruitment	Interviews
Human Resources	Recruitment	Positions
Human Resources	Recruitment	Unsuccesful Candidates
Human Resources	**Termination of Employment**	
Human Resources	**Training**	Courses
Human Resources	Training	Induction

Function	Activity	Sub Activity
Information Management	**Data Protection**	Training
Information Management	Data Protection	Registration
Information Management	Data Protection	Research & Information
Information Management	Data Protection	Breaches
Information Management	**Freedom of Information**	Research & information
Information Management	Freedom of Information	Scottish Information Commissioner
Information Management	Freedom of Information	Information Request Register
Information Management	Freedom of Information	Publication Scheme
Information Management	Freedom of Information	General Administration
Information Management	Freedom of Information	FOI Requests
Information Management	**Information Resources**	Current Awareness
Information Management	Information Resources	External Resources
Information Management	Information Resources	General Administration
Information Management	**Records Management**	Records Management Plan & Evidence
Information Management	Records Management	General Administration
Information Management	Records Management	Public Records Scotland Act 2011
Information Management	Records Management	Information Management Audit
Information Management	Records Management	Retention Schedule
Information Technology	**Systems Development**	Client Relationship Management
Information Technology	Systems Development	Filemaker - Enquiry System
Information Technology	Systems Development	Remote Access
Information Technology	Systems Development	CHAS

Function	Activity	Sub Activity
Information Technology	Systems Development	TRIM
Information Technology	**Systems Management**	HP Records Manager
Information Technology	Systems Management	TRIM Upgrade
Information Technology	Systems Management	Filemaker - Enquiry System
Information Technology	Systems Management	Administration
Information Technology	Systems Management	CHAS
Information Technology	Systems Management	TRIM
Investigations	**Enquiries**	Policies & Procedures
Investigations	Enquiries	Statistics & Performance
Investigations	Enquiries	Case Files
Investigations	**Formal**	Investigation Report & Recommendations
Investigations	Formal	Research & Information
Investigations	Formal	Correspondence
Investigations	Formal	Evidence
Investigations	**Informal**	Research & Information
Investigations	Informal	Correspondence
National Consultation	**National Consultation 2005-2006**	
National Consultation	**Right Blether 2010-2011**	
National Consultation	**Wee Blether 2012**	
Participation & Consultation	**Administration**	Finance
Participation & Consultation	Administration	Review of Work
Participation & Consultation	**Campaigns**	

Function	Activity	Sub Activity
Participation & Consultation	**CYP Working Groups**	
Participation & Consultation	**Methods of Working**	Early Years
Participation & Consultation	Methods of Working	Youth Work
Participation & Consultation	**National Consultation**	2005-2006
Participation & Consultation	National Consultation	Right Blether 2010-2011
Participation & Consultation	National Consultation	Wee Blether 2012
Participation & Consultation	**Partnership Working**	
Participation & Consultation	**Resources**	Golden Rules for Participation
Participation & Consultation	Resources	Workshop Resources
Participation & Consultation	**Strategy**	
Participation & Consultation	**Training for External Organisations**	
Policy & Parliamentary	**Briefings & Policy Positions**	External Briefings
Policy & Parliamentary	Briefings & Policy Positions	Internal Briefings
Policy & Parliamentary	Briefings & Policy Positions	Policy Position Papers
Policy & Parliamentary	**Consultations**	Responses & Evidence to Parliament (by year)
Policy & Parliamentary	Consultations	Response Process
Policy & Parliamentary	Consultations	Research
Policy & Parliamentary	**Parliamentary Work**	Bills
Policy & Parliamentary	Parliamentary Work	Inquiry / Reviews
Policy & Parliamentary	Parliamentary Work	Parliamentary Strategy
Policy & Parliamentary	Parliamentary Work	Parliamentary Update
Policy & Parliamentary	Parliamentary Work	Party Conferences

Function	Activity	Sub Activity
Policy & Parliamentary	Parliamentary Work	Public Petitions
Policy & Parliamentary	Parliamentary Work	Westminster
Policy & Parliamentary	**Policy Administration**	Policy Monitoring
Policy & Parliamentary	**Policy Development**	Sub levels arranged by key subject
Policy & Parliamentary	**Policy Prioritisation**	Policy Priorities 2009-14
Policy & Parliamentary	Policy Prioritisation	Consultation & Responses
Policy & Parliamentary	Policy Prioritisation	Research Analysis
Projects 2004-2009	**Asylum**	
Projects 2004-2009	**Being Young In Scotland**	
Projects 2004-2009	**Children & Young People Legislation**	
Projects 2004-2009	**Children in Prison**	
Projects 2004-2009	**Detective Kits**	
Projects 2004-2009	**Leaving Care**	
Projects 2004-2009	**Moving & Handling**	
Projects 2009-2017	**Child Trafficking**	
Projects 2009-2017	**Children of Prisoners**	
Projects 2009-2017	**Children and Young People Legislation**	Children and Young People Bill
Projects 2009-2017	Children and Young People Legislation	Rights of Children and Young People Bill
Projects 2009-2017	**Children and Young People (Scotland) Act**	
Projects 2009-2017	**Disability**	
Projects 2009-2017	**Domestic Abuse**	
Projects 2009-2017	**Mosquito Devices**	

Function	Activity	Sub Activity
Projects 2009-2017	**National Participation Framework & Standards**	
Projects 2009-2017	**Poverty, Education and Attainment**	
Projects 2009-2017	**School Toilets (Flushed with Success)**	
Projects 2009-2017	**Youth Football**	
Research	**Commissioning Research**	
Research	**Grant Applications**	PhD Case Studentship
Research	**Guidelines and Protocols**	Research Guidelines
Research	**Research Administration**	

Evidence 5.1: Retention Schedule

FINANCE								
ACTIVITY / RECORDS SERIES	**DESCRIPTION/EXAMPLES OF RECORD TYPES**	**TRIGGER (event that prompts start of retention period**	**RETENTION PERIOD**	**ACTION**	**CUSTODIAN**	**AUTHORITY**	**CITATION & NOTES**	**LOCATION**
ANNUAL ACCOUNTS								
Annual accounts			Permanent	Retain/NAS Transfer	HCS (Head of Corporate Services)	Statutory	Taxes Management Act 1970	TRIM/Paper
Records documenting the preparation of SCCYP's annual accounts	Audit plan, list of pre-payments, accruals, debtors, creditors	Completion of Audit	6 years	Destroy	HCS	Statutory	Taxes Management Act 1970	TRIM
Audit (Internal & External)	Final Report	End of Financial Year (on completion of audit)	6 years	Destroy	HCS	Business requirement		TRIM
Audit (Internal & External)	Interim Reports, Correspondence	End of Financial Year (on completion of audit)	6 years	Destroy	HCS	Business requirement		TRIM
Audit Advisory Board	Final Report, interim resports, minutes, correspondence	End of Financial Year (on completion of audit)	6 years	Destroy	HCS	Business requirement		TRIM
ASSET MANAGEMENT								
Asset management - Records documenting the value of SCCYP's capital assets	Fixed Asset register, Asset Management Plans	End of financial year (on completion of audit)	6 years	Destroy	HCS	Statutory	Taxes Management Act 1970; Prescription and Limitation (Scotland) Acts 1973 and 1984; Value Added Tax Act 1994; Audit Commission Act 1998	TRIM

FINANCE								
ACTIVITY / RECORDS SERIES	**DESCRIPTION/EXAMPLES OF RECORD TYPES**	**TRIGGER (event that prompts start of retention period**	**RETENTION PERIOD**	**ACTION**	**CUSTODIAN**	**AUTHORITY**	**CITATION & NOTES**	**LOCATION**
Asset management - Records documenting decisions (and authorisations) to dispose of capital assets	Fixed Asset register, Asset Management Plans	End of financial year (on completion of audit)	6 years	Destroy	HCS	Statutory	Taxes Management Act 1970; Prescription and Limitation (Scotland) Acts 1973 and 1984; Value Added Tax Act 1994; Audit Commission Act 1998	TRIM
BUDGET AND ACCOUNTS MANAGEMENT								
Annual budget - setting annual budget	Annual budget report, draft budgets, estimates	End of financial year	3 years	Destroy	HCS	Business requirement		TRIM
Budget monitoring	Records documenting the monitoring of income and expenditure against annual operating budgets, and action taken to deal with variances - Monthly Expenditure Reports	End of financial year	3 years	Destroy	HCS	Business requirement		TRIM
Bank accounts - administration	Records documenting the opening, closure and routine administration of bank accounts	Closure of account	6 years	Destroy	HCS	Business requirement		Paper (HCS Cabinet)/SAGE
Bank accounts - Records documenting standing orders, direct debits etc.		Life of instruction	6 years	Destroy	HCS	Business requirement		Paper (HCS Cabinet)

FINANCE								
ACTIVITY / RECORDS SERIES	**DESCRIPTION/EXAMPLES OF RECORD TYPES**	**TRIGGER (event that prompts start of retention period**	**RETENTION PERIOD**	**ACTION**	**CUSTODIAN**	**AUTHORITY**	**CITATION & NOTES**	**LOCATION**
Records documenting the receipt and payment of purchase invoices		End of financial year (on completion of audit)	6 years	Destroy	HCS	Statutory	Taxes Management Act 1970; HMRC 700/21	Paper (Invoice Box Files)
INSURANCE								
Policy documents and related correspondence		Termination of annual policy	5 years	Destroy	HCS	Statutory	Prescription and Limitation (Scotland) Acts 1973 and 1984;	Paper (Invoice Box Files)
PAYROLL & PENSIONS								
Payroll reports	Gross salary, employers pension contributions, employers national insurance contributions - Monthly reports	End of financial year (on completion of audit)	6 years	Destroy	HCS	Statutory	Income Tax (Employments) Regulations 1993 / 744; National Minimum Wage Regulations 1999 S.I. 1999 / 584; Taxes Management Act 1970; Prescription and Limitation (Scotland) Acts 1973 and 1984	Paper (Invoice Box Files)/HCS Outlook
Pay Awards		End of financial year	6 years	Destroy	HCS	Business Requirement		TRIM

FINANCE								
ACTIVITY / RECORDS SERIES	**DESCRIPTION/EXAMPLES OF RECORD TYPES**	**TRIGGER (event that prompts start of retention period**	**RETENTION PERIOD**	**ACTION**	**CUSTODIAN**	**AUTHORITY**	**CITATION & NOTES**	**LOCATION**
Salaries – cumulative listings		End of financial year (on completion of audit)	6 years	Destroy	HCS	Statutory	Income Tax (Employments) Regulations 1993 / 744;National Minimum Wage Regulations1999 / 584;Taxes Management Act 1970; Prescription and Limitation (Scotland) Acts 1973 and 1984	HCS Outlook/Cabinet
P45	Copy	End of financial year (on completion of audit)	6yrs	Destroy	HCS	Statutory	Taxes Management Act 1970	Paper (Personnel File)
Expenses		End of financial year (on completion of audit)	6yrs	Destroy	HCS	Statutory	Taxes Management Act 1970	Paper (Invoice Box Files)
Statutory Sick Pay scheme records		End of financial year (on completion of audit)	3 years	Destroy	HCS	Statutory	Statutory Sick Pay (General) Regulations 1982 / 894	Paper (Personnel File)/Secure area of shared drive
Statutory Maternity Pay scheme records		End of financial year (on completion of audit)	3 years	Destroy	HCS	Statutory	The Statutory Maternity Pay (General) Regulations 1986 / 1960	Paper (Personnel File)/Secure area of shared drive

FINANCE								
ACTIVITY / RECORDS SERIES	**DESCRIPTION/EXAMPLES OF RECORD TYPES**	**TRIGGER (event that prompts start of retention period**	**RETENTION PERIOD**	**ACTION**	**CUSTODIAN**	**AUTHORITY**	**CITATION & NOTES**	**LOCATION**
PROCUREMENT								
CONTRACT MANAGEMENT								
Contract management - key records	Final contract, contract extensions and amendments, reports from contractors, surveys and inspections, complaints, payment disputes, minutes and papers of meetings	After contract expires	5 years	Destroy	HCS	Statutory & Vital	Prescription and Limitation (Scotland) Act 1973. These may be used for reference when preparing future related tenders	TRIM/Paper
NON-TENDERED PROCUREMENT								
Non-tendered procurement	Quotes and related correspondence - successful	End of contract	6 years	Destroy	HCS	Statutory	Prescription and Limitation (Scotland) Act 1973	Paper (Invoice Box Files)
	Internal requisition, delivery notes	End of financial year	6 yrs	Destroy	HCS	Business requirement		Paper (Invoice Box Files)
	Credit notes, invoices	End of financial year (on completion of audit)	6 yrs	Destroy	HCS	Statutory	Taxes Management Act 1970	Paper
TENDERING								
Initial proposal	Business case; contract advertisement, statements of interest (successful); draft and agreed specification, evaluation criteria, invitation to tender	End of contract	5 years	Destroy	HCS	Statutory	Prescription and Limitation (Scotland) Act 1973. Keep in contract file once contract awarded	TRIM
Tenders - unsuccessful	Includes statements of interest, tender document, tender responses	Award of contract	1 year	Destroy	HCS	Business requirement		TRIM

FINANCE								
ACTIVITY / RECORDS SERIES	**DESCRIPTION/EXAMPLES OF RECORD TYPES**	**TRIGGER (event that prompts start of retention period**	**RETENTION PERIOD**	**ACTION**	**CUSTODIAN**	**AUTHORITY**	**CITATION & NOTES**	**LOCATION**
Tenders - successful	Includes tender document, tender responses	End of contract	5 years	Destroy	HCS	Statutory	Prescription and Limitation (Scotland) Act 1973. It is important that a record of all contracts and related transactions is kept. The files must contain a complete and accurate record of all internal and external documentation so that the stages and reasoning of the transactions are apparent.	TRIM

INVESTIGATIONS								
ACTIVITY / RECORDS SERIES	**EXAMPLES OF RECORD TYPES**	**TRIGGER**	**RETENTION PERIOD**	**ACTION**	**CUSTODIAN**	**AUTHORITY**	**CITATION/NOTES**	**LOCATION**
Enquiries & Investigations								
Enquiries & Investigation Case File	Electronic Case File: inc. case notes, correspondence, full set of evidence.	Case Closure	3 years	Destroy	HPL (Head of Policy)	Business Requirement	Enquiries Procedures	Filemaker
	Electronic Case File - Child Protection referral.	Date of birth of child	100 years	Destroy	HPL	Business Requirement	Scottish Council on Archives (SCA). Children & Family Services Retention Schedule	Filemaker
	Electronic Case File - child protection concern not referred.	Case Closure	5 years	Destroy	HPL	Business Requirement	SCA. Children & Family Services Retention Schedule	Filemaker
	Electronic Case File - Public Interest Disclosure Act 1998 (PIDA).	Case Closure	5 years	Destroy	HPL	Business Requirement	Whistleblowing Procedures	Filemaker
	Paper Case File.	Case Closure	3 months	Destroy (Confidential Waste)	HPL	Business Requirement	Enquiries Procedures	Enquiries - Locked Cupboard
	Investigation Report	Issue of Final Report	Permanent	Retain	HPL	Business Requirement	Enquiries Procedures	TRIM
	Investigation Recommendations	Issue of Recommendations	Permanent	Retain	HPL	Business Requirement	Enquiries Procedures	TRIM
Performance Reporting								
Statistics	Annual Statistics Report	End of Enquiry Year	Permanent	Retain	HPL	Business Requirement	Enquiries Procedures	TRIM

Evidence 6.1: UKSSA Certificate of Compliance of Confidential Waste Contractor

UKSSA United Kingdom Security Shredding Association

Certificate of Compliance

THIS IS TO CERTIFY THAT

Changeworks Recycling Ltd
36 Newhaven Road
Edinburgh
EH6 5PY

WAS SUCCESSFULLY VETTED TO THE UKSSA CODE OF PRACTICE INCORPORATING BS EN 15713:2009 AND BS 7858:2012 STANDARDS ON

6th November 2014

SIGNED:
SECRETARY UKSSA

VALID UNTIL: 5th November 2016

UKSSA
UNITED KINGDOM SECURITY SHREDDING ASSOCIATION

Your assurance of security in shredding

Evidence 6.2: UKSSA Code of Practice

UKSSA
UNITED KINGDOM
SECURITY SHREDDING ASSOCIATION

CODE OF PRACTICE

This code of practice lays down the aims and objectives of the United Kingdom Security Shredding Association, the standards of service with which the association's members should comply. It provides members with clear guidelines for operation and members' customers with the assurance required to select security-shredding and confidential data destruction services with absolute confidence.
Any enquiries relating to this code of practice should be made to UKSSA via the Association website www.ukssa.org.uk.

1. NAME
The name of the association is the:
'UNITED KINGDOM SECURITY SHREDDING ASSOCIATION'.
Hereafter also referred to as UKSSA or 'the Association'.

2. AIMS AND OBJECTIVES
i) To collectively promote members' security shredding and confidential data destruction services at local and national levels.
ii) Offer member services for the secure destruction of all data including paper, tape, acetate, film and electronic media.
iii) Have a broad membership to ensure effective representation of all areas of the United Kingdom and Ireland.
iv) Ensure that members are committed to offering a service that is appropriate to customers' requirements.
v) Offer advice and assistance to external organisations requiring disposal and destruction of confidential documents and data.
vi) To rigorously enforce the standards set by the Association across all members.
vii) Establish and maintain high standards of service and performance throughout the security shredding industry.
viii) Liaise with government and other legislative, authoritative and regulatory bodies at local, national and international levels to establish, maintain, improve and enforce the highest standards of operation and best practice throughout the industry.

3. STANDARDS

3.1. COMPLIANCE
All members must comply with the requirements of the UKSSA Code of Practice, the Data Protection Act, BS EN 15713 and BS 7858.

Where there is a conflict, the UKSSA Code of Practice will take precedence.

United Kingdom Security Shredding Association Heritage House Vicar Lane Daventry Northants NN11 4GD
Tel: 0800 634 0212 admin@ukssa.org.uk ukssa.org.uk

3.2. BUILDING SECURITY

i) The destruction process must be in secure isolation from any other processing.
ii) Buildings must be of a secure nature and have high security locks with restricted access to unauthorised personnel at all times.
iii) All unprocessed material must be stored in secure facilities.
iv) Buildings should comply with all relevant fire and safety regulations.
v) Buildings involved in the destruction or storage of confidential material must be alarmed.
vi) Premises must have full time closed circuit television monitoring systems and/or an appropriate level of on-site security personnel, and must comply with the current Data Protection Act.

3.3 SECURE COLLECTION CONTAINERS

i) All containers used must be lockable or sealable.
ii) Numbered seals will be provided on customer request.

3.4 MOBILE SHREDDING OPERATIONS

Where a member operates mobile shredding units, the confidential material should not be moved to facilities that are remote from the client's location. Vehicles should meet the following requirements:

i) Vehicles must be clean and presentable at all times.
ii) Vehicles must have a rigid box body.
iii) Vehicles must be fitted with lockable and/or sealable doors.
iv) Vehicles must be capable of communicating with base during operation.
v) Vehicles must not be left unattended when unprocessed confidential material is on board.
vi) Vehicles must be fitted with an insurance approved immobilising device that functions whilst material is being processed.
vii) Vehicles must conform to the shred size as set out in 3.7 SHREDDING, below

3.5 TRANSPORT

i) Vehicles must be clean and presentable at all times.
ii) Vehicles must have a rigid box body or secure container capable of accommodating all security sensitive materials.
iii) All vehicle doors must be lockable and vehicle bodies sealable.
iv) Vehicles must not be left open or unlocked whilst unattended, keys must never be left in the vehicle.
v) Vehicles must be capable of communicating with base during operation.
vi) Vehicles must be fitted with an alarm or immobiliser.
vii) Sub-contractors must comply with UKSSA standards at all times. It is the duty of the member to ensure sub-contractor conformity.

3.6 SECURITY & AUDIT TRAIL

Material collections and deliveries will be documented at all stages of the process, through to the issue of a Certificate of Destruction after the material has been shredded, to provide an audit trail as clear proof of service completion.

A contract must exist between the data controller and the processor in line with the requirements of the Data Protection Act Regulations.

3.7 SHREDDING

All members must have the availability of shredding equipment to meet the following:

i) Shred size of no greater than 22mm OR total destruction
ii) Members should ensure <u>all</u> material is destroyed within 24 working hours of collection.

United Kingdom Security Shredding Association Heritage House Vicar Lane Daventry Northants NN11 4GD
Tel: 0800 634 0212 admin@ukssa.org.uk ukssa.org.uk

3.8 PERSONNEL

i) Members must ensure their integrity by vetting employees directly involved in any aspect of their shredding/destruction operation to BS 7858.
ii) Personnel must have received the necessary training and hold appropriate qualifications to ensure they are competent in all aspects of their work.
iii) Identity passes must be issued and worn by all employees at all times. Passes should include a recent photograph of the employee, employee's name, position, company name and contact telephone number. Passes should bear an expiry date of no greater than 3 years.
iv) Drivers must be suitably attired with smart safety clothing.
v) All personnel involved in the security shredding and/or confidential data destruction departments of the business must have signed a confidentiality agreement.

3.9 INSURANCE

i) All members must have a minimum £5,000,000 public & products liability and £10,000,000 employers' liability insurance.

3.10 INSPECTIONS

i) Members will subject themselves to vetting by an UKSSA appointed independent security consultant to ensure compliance with UKSSA standards. Upon successful completion a Certificate of Conformity will be issued.
ii) Members must be compliant with the current Data Protection Act and BS EN 15713.
iii) Members must be registered with the Environmental Agency under the Duty of Care Waste Regulations.
iv) Any member holding national contracts has the right to inspect sub-contractor members at any time.
iv) Members must provide the facility for customers to inspect all security shredding facilities at mutually convenient times.

3.11 ENVIRONMENTAL CARE

i) All shredded material should be disposed of in an environmentally responsible manner.
ii) All processes should have as little detrimental impact on the environment as possible.

4. MANAGEMENT

The management of affairs of the Association shall be vested in an Executive Council consisting of:

i) Chairman, Vice Chairman, Treasurer and Secretary.
ii) All full members and/or their representatives.
iii) The Chairman, Vice Chairman, Treasurer and Secretary will be elected annually from among full members of the Association and the term of office shall be one year.

5. PROCEEDINGS

i) The Association Executive Council shall meet monthly, or at such intervals as may be convenient for the relevant business dealings and meetings shall be held at places determined by the Executive Council.
ii) The quorum for the Executive Council's business shall be not less than 50%.
iii) At such meetings, each fully accredited member shall have one vote and all resolutions and decisions of the Executive Council shall be made by a simple majority of votes cast. In the event of a tied vote, the chairman of the meeting shall hold the casting vote.

United Kingdom Security Shredding Association Heritage House Vicar Lane Daventry Northants NN11 4GD
Tel: 0800 634 0212 admin@ukssa.org.uk ukssa.org.uk

6. MEMBERSHIP

i) To have qualification, members must be actively involved in the process of security shredding and have facilities available to meet the standards as set out by the Executive Council.
ii) Members may only be elected or expelled with the full agreement of the Executive Council.
iv) Members may resign from the Association at any time by giving 6 months written notice. There will be no refunding of membership/audit fees upon resignation or expulsion.
v) Any person or corporate body wishing to join the Association must hold the necessary qualifications and have two full Association members to propose and second any nomination in writing to the Chairman or Treasurer.
v) The Association, at its discretion, may determine the maximum number of members of UKSSA and declare membership closed whenever it may think fit.

7. PROMOTION

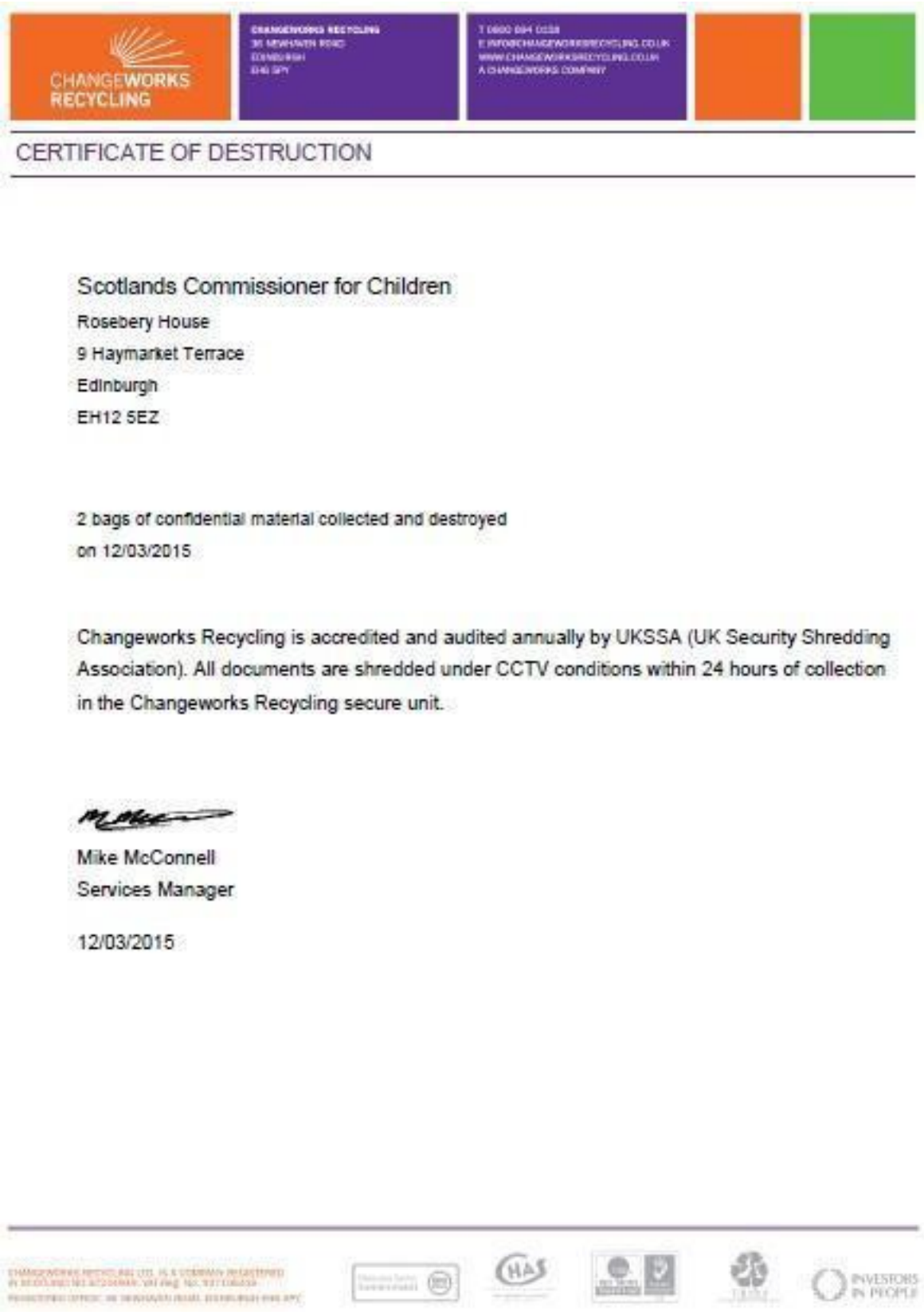
i) Only fully accredited members will be able to declare or represent themselves as members of the Association.
ii) Only fully accredited members will be able to use the Association logo, namestyle, literature or other forms of communication.
iii) Only fully accredited production locations will be listed on the UKSSA website.
iv) Members should not use the UKSSA logo, namestyle, literature or other forms of communication to imply that member operations are fully accredited to UKSSA unless each operation is fully accredited to the UKSSA Code of Practice through independent audit.
v) Any member acquiring a new security shredding operation should not imply that this operation is fully accredited to the UKSSA Code of Practice under their Membership of UKSSA until an independent audit of the new operation has been carried out against the UKSSA Code of Practice.
vi) Any Member acquiring a new security shredding operation that has already been fully accredited to the UKSSA Code of Practice through independent audit can continue to imply that the operation is fully accredited to the UKSSA Code of Practice dependent on the frequency of audit for that operation being maintained in line with the UKSSA Code of Practice.
vii) Fully accredited Members should not use the UKSSA logo, namestyle, literature or other forms of communication to monopolise internet search engine listings.

8. AMENDMENTS TO THE RULES

i) These rules may be modified, varied or supplemented as necessary by the Executive Council in the Association meetings.

United Kingdom Security Shredding Association Heritage House Vicar Lane Daventry Northants NN11 4GD
Tel: 0800 634 0212 admin@ukssa.org.uk ukssa.org.uk

Evidence 6.3: Certificate of Destruction (Example)



CHANGEWORKS RECYCLING

CERTIFICATE OF DESTRUCTION

Scotlands Commissioner for Children
Rosebery House
9 Haymarket Terrace
Edinburgh
EH12 5EZ

2 bags of confidential material collected and destroyed
on 12/03/2015

Changeworks Recycling is accredited and audited annually by UKSSA (UK Security Shredding Association). All documents are shredded under CCTV conditions within 24 hours of collection in the Changeworks Recycling secure unit.

Mike McConnell
Services Manager

12/03/2015

Evidence 6.4: IT Recycling & Data Destruction Services 2015-2016

Dunedin

Dunedin IT

Recycling &

Data Destruction Services

2015-2016

2014-2

22 Young Street Lane North, Edinburgh, EH2 4JD. Scotland
Office Tel : 0131 225 2215
Registered Company No : SC364906 VAT No : 976927648

Dunedin

Table of Contents

Dunedin

Dunedin IT are fully ISO 9001 compliant and our client services, contact procedures, processes and IT settings are audited internally on quarterly basis and externally by a fully accredited company who perform a full annual ISO 9001 audit. We offer our clients the following IT Recycling and Destruction services which and are fully documented within our Quality Procedures and form part of our ISO 9001 documentation.

Dunedin IT-Recycling & Data Destruction Services

What we do

Dunedin IT aims to offer our clients the most secure, flexible and cost-effective collection, data destruction and recycling services within Scotland. We partner with a recycling company, who are fully aware of our clients' responsibilities under the Data Protection Act 1998. By partnering with a IT recycling specialist, we can offer a quality guaranteed and certified data destruction service, by either wiping or physically destroying the items containing such data, but we ensure security from the time of collection through to destruction.

Why do we do this

The Data Protection Act 1998 applies to all personal data whether it's about your clients or employees and applies to all personal data as minor as phone numbers and addresses.

All companies holding personal data relating to employees and/or customers are responsible for complying with The Data Protection Act 1998. The Act states that companies have a duty of care to ensure that such data is kept confidential and does not leak into the public domain.

Our Recycling Partner

Dunedin IT use an Edinburgh-based IT Recycling company specialising in Data Destruction and Equipment Resale to businesses small and large throughout the UK. Dunedin IT have chosen to partner with Pure IT, as they can offer most **secure, flexible** and **cost-effective Recycling** and **Data Destruction service** in Scotland and are fully licensed by the Scottish Environmental Protection Agency (SEPA) to ensure their processes cover legal responsibility under the European Waste Electrical

and Electronic Equipment (WEEE) Directive, the Restriction of Hazardous Substances (RoHS) Directive and the Data Protection Act 1998.

Destruction Services we offer

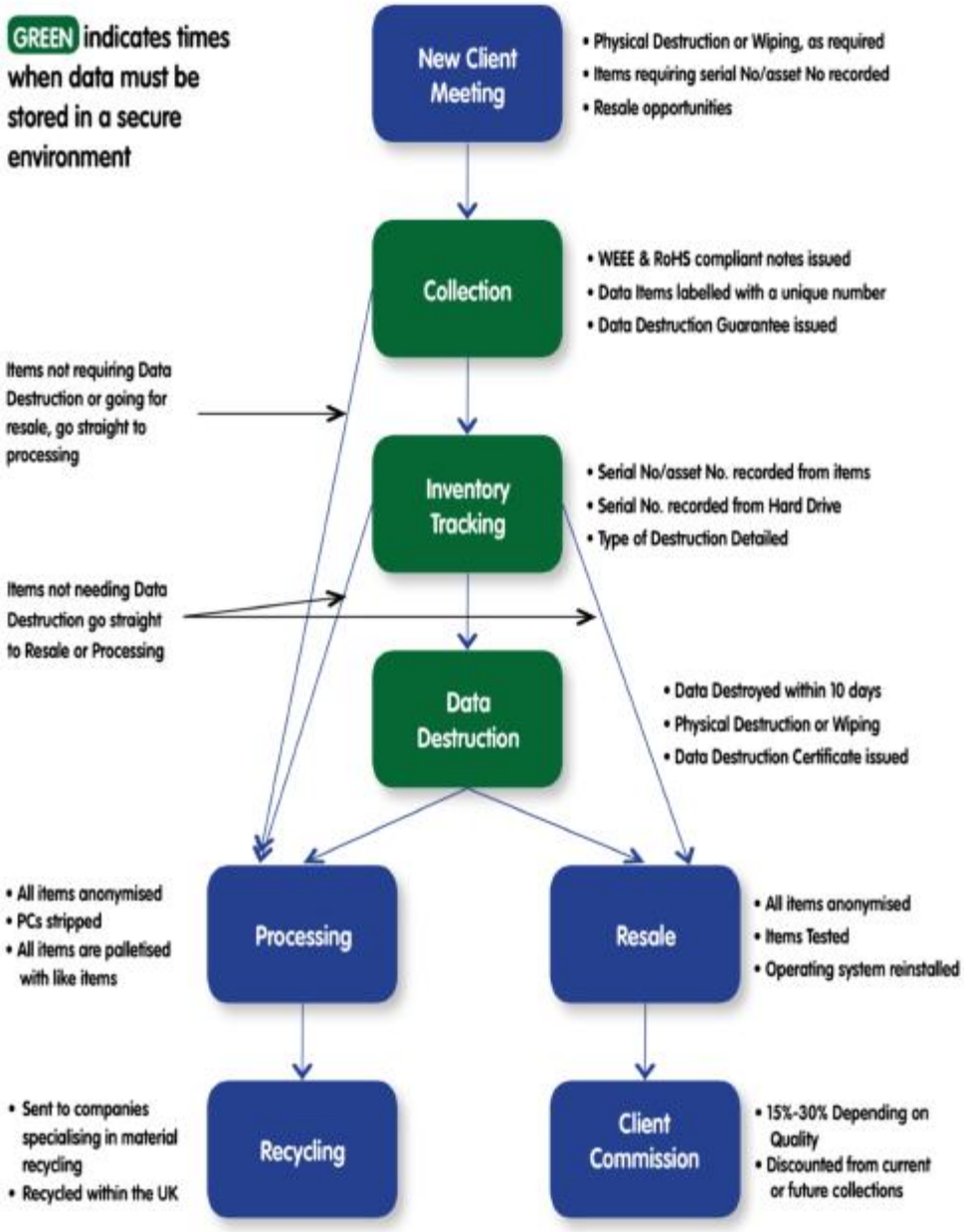
- Destruction of PC and Server hard drives, data-back up tapes, PDA's and other data storage devices.
- Guaranteed Data Destruction
- Physical destruction or data wiping to US standard DOD 5220.2-M
- Audit Trail for transparency (including serial no, asset no, model, type of destruction)
- Certificate issued after destruction
- Secure collection service
- Bespoke destruction service

Our Procedure & Policy Governance Process Flow

The following process flow diagram explains the processes and procedures that we undertake when completing IT Equipment disposal.

Dunedin

Dunedin IT
Equipment Disposal & Recycling Process



22 Young Street Lane North, Edinburgh, EH2 4JD. Scotland
Office Tel : 0131 225 2215
Registered Company No : SC364906 VAT No : 976927648

Dunedin

Our Certification

QAS International

REGISTRATION CERTIFICATE

This document certifies that the administration systems of

Dunedin IT Ltd

22 Young St North Lane, Edinburgh EH2 4JD

have been assessed and approved by QAS International to the following management systems, standards and guidelines:

ISO 9001 : 2008

With the permitted exclusion of clause 7.6 Control of Monitoring and Measuring Equipment

The approved administration systems apply to the following:

Consultancy, Network Design and IT Support Services.

Original Approval	*30th June 2014*
Current Certificate	*30th June 2014*
Certificate Expiry	*30th June 2015*
Certificate Number	*A14496*

Signed: Certification Officer

On behalf of QAS International

This certificate remains valid while the holder maintains their quality administration systems in accordance with the standards and guidelines stated above, which will be audited annually by QAS International. The holder is entitled to display the above registration mark for the duration of this certificate, which should be returned to QAS International upon reasonable request. Issuing Office: QAS International, 20A Oxford Street, Malmesbury, Wiltshire SN16 9AX, UK

QAS INTERNATIONAL

Evidence 6.5: IT Data Destruction Certificate (Sample)

Appendix B – Sample Certificate of Data Destruction

Certificate of Data Destruction / Wiping

Reselling & Recycling
Secure Date Destruction

This is to certify to .....

that the data on the hard drives identified on the attached pages identified as .....

has been physically destroyed or wiped to US standard DoD 5220.22-M

By

Pure IT Recycling Ltd

Signed on behalf of Pure IT Recycling Ltd:_____(Director) Date:_____

Pure IT Recycling Ltd, 14 Riversdale Crescent, Edinburgh, EH12 5QT.
Company Registration Number: SC329414 : Waste Carriers Licence No: SCO/046558
www.pureitrecycling.co.uk
Tel: 0131 337 9298

22 Young Street Lane North, Edinburgh, EH2 4JD. Scotland
Office Tel : 0131 225 2215

Registered Company No : SC364906 VAT No : 976927648

Evidence 6.6: IT Support Contract (section on data destruction services)

Dunedin

Dunedin IT Limited
IT Support Contract Terms & Conditions

For

SCCYP
Scotland's Commissioner for Children & Young People

2015

analyse Support monitor evolve

4.2	Unlimited remote access support for fault diagnosis	Yes
4.3	Problem resolution where possible	Yes
4.4	Access to 2nd level support staff for technical advice	Yes
5	**Additional Level One Extras**	
5.1	Inventory management [Asset Register]	Yes
5.2	IT Handbook	Yes
5.3	Password Database	Yes
6	**Additional Services**	
6.1	Off-site backup	Yes
6.2	Disaster Recovery [In conjunction with 3rd Parties]	Yes
6.3	External Comms links/Internet Broadband	Yes
6.4	Web & Email Hosting [Email Hosting only]	Yes
6.5	Proactive Server & Network monitoring	Yes
6.6	Hosted Web Apps[In support of supplier]	Yes
7	On-site support – Outside of the IT support contract, agreed before hand	
7.1	Ad-hoc visits on an 'as and when required' basis at a discounted hourly rate for **SCCYP**: On-site Discounted Rate [Mon to Fri 08:30-20:30]	£55.00
7.2	Out Of Hours Charges [20:30 to 00:00], charged at Discounted rate :	£55.00
7.3	Out Of Hours Charges[00:00 to 08:30], charged at Discounted rate:	£65.00
7.4	Weekend[Sat & Sun] hourly rates, charged at discounted rate.	**Contracted**

Dunedin IT Recycling & Data Destruction Services

Dunedin IT will contract with our partner[Pure IT recycling], whom we will use for specialised Data Destruction for/and on behalf of SCCYP for any requirement for data destruction services on any redundant electrical equipment. Pure IT are licensed by the Scottish Environmental Protection Agency [SEPA] to ensure their processes cover our legal responsibility under the European Waste Electrical and Electronic Equipment [WEEE] Directive, the Restriction of Hazardous Substances [RoHS] Directive and the Data Protection Act 1998.

The Destruction of PC and Server hard drives, data-back up tapes, PDA's and other data storage devices will be provided via a Guaranteed Data Destruction service which covers the Secure pick up of equipment, the Physical destruction or data wiping to US standard DOD 5220.2 – M. Dunedin IT will provide a full Audit Trail for transparency [including serial no, asset no, model, type of destruction] and once destruction is complete a Certificate will be issued after destruction. A sample of said Certificate can be found in Appendix B of this contract. This service will be provided on a "as and when required basis", with SCCYP charged on a time and materials basis

22 Young Street Lane North, Edinburgh, EH2 4JD. Scotland
Office Tel : 0131 225 2215

Registered Company No : SC364906 VAT No : 976927648

6 SUPPORT CONTRACT TERMS & CONDITIONS OF BUSINESS

On acceptance by you the following terms and conditions will form a legally binding contract between us.

CLIENT:	*SCCYP*
COMMENCEMENT DATE:	1st April 2015
CONTRACT TERM:	12 Months
CANCELLATION PERIOD:	*90 Days written notice*

1. Support Services

1.1 In consideration of the payment of the fee Dunedin IT Limited undertake to provide support services providing for the diagnosis of defects or errors in such specified hardware or software as are agreed between the parties in writing.

1.2 Telephone support will be provided upon request between the hours of **08:30 and 17:30 Monday through Friday** (excluding 25th, 26th and 31st December and 1st and 2nd January). Other public holidays include Easter Monday and Bank holidays (Where agreed) there will be reduced staff.

1.3 Where support is required to be carried out at your premises, Dunedin IT Limited will provide such support at such times during normal business hours as shall be agreed between us. All associated costs properly and reasonably incurred by us in relation to support carried out at your premises will be paid by you in addition to the fee.

1.4 Support services provided at your premises may result in a recommendation being made by Dunedin IT Limited that further work/services be carried out on your behalf that are outwith the ambit of this support contract. In these circumstances Dunedin IT Limited will provide you with full details of the additional work recommended and associated fees/costs and in the event that you instruct us to carry out the additional work you will be responsible for all fees/costs in this respect.

1.5 Where there is a requirement for work to be carried out by third party contractors such as hardware, software or cabling engineers, Dunedin IT Limited will provide recommendations of suitable contractors that will be subject to approval by you. All work carried out will be instructed directly by you to the relevant contractor and you will be bound by the terms and conditions of the particular contract and fully responsible for all costs

22 Young Street Lane North, Edinburgh, EH2 4JD. Scotland
Office Tel : 0131 225 2215

Registered Company No : SC364906 VAT No : 976927648

11. Entire Agreement

Dunedin IT Limited shall not be liable for loss arising from any representations or statements made prior to the date of this agreement other than such as are confirmed by Dunedin IT Limited in writing.

12. Law

This agreement shall be governed by and construed in accordance with Scots law and the parties hereto agree to submit to the non-exclusive jurisdiction of the Scottish Courts: IN WITNESS WHEREOF these presents and the attached proposal are signed:-

For and on behalf of Dunedin IT Limited at Young Street North Lane, Edinburgh on the day of

.....
David Inglis or Jamie Clague

For and on behalf of :
SCCYP
85 Holyrood Road
Edinburgh
EH8 8A

.....
[Legal Signatory on behalf of SCCYP]

22 Young Street Lane North, Edinburgh, EH2 4JD. Scotland
Office Tel : 0131 225 2215

Registered Company No : SC364906 VAT No : 976927648

Evidence 7.1: Memorandum of Understanding between the Keeper and the Commissioner

MEMORANDUM OF UNDERSTANDING

Between

THE KEEPER OF THE RECORDS OF SCOTLAND

and

THE COMMISSIONER FOR CHILDREN AND YOUNG PEOPLE IN SCOTLAND

INTERPRETATION

1. In this Memorandum of Understanding, unless the context otherwise requires, the following words and phrases shall have the following meanings:

-the Commissioner means the Commissioner for Children and Young People in Scotland

-DPA 1998 means the Data Protection Act 1998

-EI(S) Regulations 2004 means the Environmental Information (Scotland) Regulations 2004

-FOISA 2002 means the Freedom of Information (Scotland) Act 2002

-the Keeper means the Keeper of the Records of Scotland

-MoU means this Memorandum of Understanding between the Keeper and the Commissioner

-NRS means National Records of Scotland

-PR Act 1958 means the Public Records Act 1958

-PR(S) Act 1937 means the Public Records (Scotland) Act 1937

-PR(S) Act 2011 means the Public Records (Scotland) Act 2011

PURPOSE

2. This MoU sets out the understanding between the Keeper and the Commissioner on how the process of depositing, storing and accessing records of enduring historical, cultural and research value which have been transferred from the Commissioner to NRS will operate. Deposit in NRS is pursuant to section 5 of the PR(S) Act 1937 and in fulfilment of the Commissioner's record management obligations under the PR(S) Act 2011.

BACKGROUND

3. The Keeper is responsible to the Scottish Ministers for records transmitted to him under various statutory provisions including the PR(S) Act 1937 and section 3 of the PR Act 1958, as well as for records of the courts and those of independent origin selected for permanent preservation. The Keeper's functions are carried out by NRS, as a Non-Ministerial Department forming part of the Scottish Administration. NRS preserves Scotland's national archives so that they are available for current and future generations; it registers births, marriages, civil partnerships, deaths, divorces and adoptions; it operates the census; it publishes information about Scotland's population and households; it maintains the National Health Service Central Register; and it connects people of Scots ancestry with their past.

4. The Commissioner for Children and Young People in Scotland was established by an Act of the Scottish Parliament in 2003. The Commissioner is an individual appointed by Her Majesty on the nomination of the Scottish Parliament. The Commissioner is responsible for promoting and safeguarding the rights of all children and young people in Scotland under the age of 18, and those under the age of 21 if they have at any time been in the care of, or looked after by a local authority. In doing so the Commissioner must promote awareness and understanding of the rights of children and young people; keep under review law, policy and practice relating to the rights of children and young people; promote best practice by service providers; and promote, commission, undertake and publish research on matters relating to the rights of children and young people.

STATUTORY FRAMEWORK

5. Section 5(1) of the PR(S) Act 1937 states that "*It shall be lawful for any Government Department, board of trustees, or other body or person having the custody of any records belonging to His Majesty and relating exclusively or mainly to Scotland (other than the documents specified in section four of this Act) to transmit such records to the Keeper.*"

6. The Commissioner is listed in the Schedule to the PR(S) Act 2011 as an authority to which Part 1 of the Act applies. The PR(S) Act 2011 obliges the Commissioner to manage its public records in accordance with a records management plan, agreed with the Keeper, which includes provision for identifying and transferring records of enduring value to an appropriate archive repository.

RECORDS TRANSFERRED TO THE KEEPER, OWNERSHIP AND TERMS OF DEPOSIT

7. The records referred to in this MoU are the Commissioner's records of enduring value which are worthy of permanent preservation for their historical, cultural and research value, as determined by the Keeper and in agreement with the Commissioner. The records can be in any format, including paper and electronic.

8. The Keeper agrees to the deposit of the Commissioner's records on behalf of the Scottish Ministers under section 5 of the PR(S) Act 1937 as a collection of national importance, and in fulfilment of the Commissioner's records management obligations under the PR(S) Act 2011.

9. Ownership of the records rests with the Commissioner.

RESPECTIVE OBLIGATIONS, PUBLIC ACCESS AND FURTHER USE

10. The Commissioner agrees to provide the Keeper with access to its record stores to facilitate identification, appraisal and selection of records considered worthy of permanent preservation in NRS.

11. The Commissioner agrees to ensure that records are properly managed to enable appraisal and processing by NRS staff.

12. The Commissioner agrees to ensure that any classified records selected for transfer to the Keeper have been declassified, with all protective markings removed from documents, prior to transmission to the Keeper.

13. The Commissioner agrees to inform the Keeper at the time that the records are transmitted to NRS of any restrictions on public access to records enforced under the DPA 1998, FOISA 2002, and the EI(S) Regulations 2004.

14. Where electronic records are deemed worthy of permanent preservation in NRS by the Keeper, the Commissioner agrees to work with NRS in order to fulfil the requirements of the NRS Deposit Agreement for Electronic Records (2013).

15. The Keeper may refuse to accept for preservation records in any format which: have poor explanatory documentation or metadata; are in poor physical condition or are digitally degraded/contaminated; are disordered or disbound, especially where it is impossible to establish the original order with any certainty; or which are not considered suitable for permanent preservation, e.g. published information, library material and records still considered to be current or semi-current. These will remain in the custody of the Commissioner.

16. The Keeper will place the catalogue of the Commissioner's record information onto the NRS online electronic catalogue to permit public access to, and facilitate use of, the records in the collection. The catalogue will comply with the DPA 1998.

17. Where possible, NRS will handle general public enquiries about the records transferred to the Keeper. These will form part of the normal NRS search room service. If required, the Commissioner will supply the Keeper with sufficient advice, information, or training to permit NRS to deal effectively with such general enquiries.

18. Enquiries of a more complex nature may be referred to the Commissioner. In this context, the temporary return ("retransmission") of specific records under section 5(3) of the PR(S) Act 1937 to the Commissioner will only be undertaken should it prove impossible for NRS staff to deal adequately with enquiries or for the client to deal with them in an alternative way (eg by NRS providing digital copies).

19. The Commissioner's records transferred to the Keeper are subject to FOISA 2002. The Keeper will administer requests for information in transferred records which are not open as stipulated under section 22 of FOISA 2002. The Keeper will refer requests to the Commissioner who will advise the Keeper of the Commissioner's decision in accordance with sections 22(2) and 22(3) of FOISA 2002. The Keeper will refer any requirements for review of the Commissioner's decisions to the Commissioner, which will review the decision and inform the Keeper of the outcome, including a statement of its reasons, in accordance with sections 22(4) and 22(5) of FOISA 2002. The Commissioner must advise the Keeper of decisions and review outcomes promptly and in any event within sufficient time to make it practicable for the Keeper to respond within the statutory 30-working-day deadlines as stipulated under sections 10(2) and 21(2) of the FOISA 2002.

20. The Commissioner's records transferred to the Keeper are subject to the EI(S) Regulations 2004. The Keeper will administer requests for access to environmental information contained in transferred records which are not open made under regulation 5(1) of the EI(S) Regulations 2004, and representations for a review made under regulation 16 of the EI(S) Regulations 2004. The Keeper will refer requests and representations for review to the Commissioner, who will advise the Keeper of the Commissioner's decision in accordance with regulations 15 and 16 of the EI(S) Regulations 2004. The Commissioner will advise the Keeper of the decision or review outcome within sufficient time to make it practicable for the Keeper to respond within the statutory 20-working-day deadlines as stipulated under regulations 5(2)(a) and 16 of the EI(S) Regulations 2004. The 20-day time period for responding to requests can be extended to 40 days where the information requested is complex and voluminous, per regulation 7 of the EI(S) Regulations 2004.

21. The Commissioner remains the data controller (as defined in section 1(1) of the DPA 1998) of all personal information transferred to the Keeper. NRS will be the data processor (as defined in section 1(1) of the DPA 1998) of this information and administer any subject access requests under section 7 of the DPA 1998 to closed Commissioner personal information. The Keeper will refer the request to the Commissioner, which will advise the Keeper of its decision within sufficient time to make it practicable for the Keeper to respond

to the request within the statutory 40 day deadline as stipulated under section 7 of the DPA 1998.

22. The Keeper will retransmit records which are necessary for the Commissioner's business purposes on request, under section 5(3) of the PR(S) Act 1937. Arrangements for collection and return of such records shall be the responsibility of the Commissioner. The Keeper agrees to make records available for collection by the Commissioner within 2 working days of receipt of a request for retransmission. Retransmitted records in the custody of the Commissioner will be handled with care, in accordance with the NRS 'Information and Regulations for Retransmitted Files'. The Commissioner must return records to the Keeper as soon as they have ceased to be required.

23. Records created by the Commissioner are subject to private copyright and the copyright holder is the Commissioner. The Commissioner must identify any third-party copyright material present in records selected for transfer and, where possible, details of the copyright owner should accompany the transfer of this material. The Keeper will manage the Commissioner's transferred records in accordance with UK copyright legislation.

24. To the extent that the Commissioner holds the copyright to the material, the Commissioner grants the Keeper a non-exclusive, world-wide and royalty free licence to use the records for any purpose which the Keeper may deem suitable in line with NRS strategic aims and for improvement of public access to the records. This may include use for any publicity, marketing or educational initiatives, and include the creation of surrogate digital images to answer public enquiries, for use in NRS search rooms and the ScotlandsPeople Family History Centre, or for use on partner websites operated with others including ScotlandsPeople and ScotlandsPlaces. The Keeper may, in accordance with section 10 of PR(S)A 1937 and any Acts of Sederunt made thereunder, charge for certain types of access, e.g. supply of digital images or copies in paper form.

25. Where a dispute occurs between the Keeper and the Commissioner, the staff who have been involved from the respective organisations should make attempts to affect a resolution, involving line management where a resolution has not been found. For ongoing disputes, the organisations' Chief Executives will work together to effect a resolution.

REVIEW OF MoU

26. Ad hoc amendments to this MoU can be made in writing, with the agreement of both parties at any time, with the provision of 2 months advance notice.

27. Formal review of the MoU should take place every 3 to 5 years.

Signature for the Commissioner	Signature on behalf of The Keeper
Signed: Tam Baillie	**Signed:** L. h. Mitchell
Name: Tam Baillie	**Name:** Laura Mitchell
Position: Commissioner for Children and Young People in Scotland	**Position:** Deputy Keeper of the Records of Scotland
Date: 10/07/15	**Date:** 5/8/15

Remote Working Policy

Table of Contents

1 Introduction

This policy applies to all staff that use or remotely access work-related information. It applies to all staff working from home. Remote working presents significant risks for the Commissioner and their office. There is a greater risk to information while in transit from remote locations to the Commissioner's office. There can be a greater risk of unauthorised access to information and loss or destruction of data. When you are remote working you will be responsible for the security and safekeeping of work-related information and office equipment in your care. To ensure that all staff processing information remotely do so securely and also in accordance with the Data Protection Act 1998, the Commissioner has developed this policy.

2 Authorisation

Where a member of staff needs to remotely access sensitive personal information as part of their work they must be authorised to do so by the Head of Corporate Services. Sensitive personal data is information concerning a living individual's racial or ethnic origins, political opinions, religious beliefs, membership of a trade union, physical or mental health, sexual life and criminal records. A written remote working agreement should regulate how the member of staff works remotely and include provisions for secure access. As part of the remote working agreement, a risk assessment should be conducted before the remote working begins. The risk assessment should consider the following:

- The sensitivity of the information to be processed;
- the security of the equipment to be used;
- the suitability of the proposed location for remote working; and
- the most secure way of working in the context.

The Head of Corporate Services must ensure that members of staff working remotely are aware of their responsibilities under the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002.

3 Precautions

All staff should take sensible precautions to protect against the loss or interference with all work related information. Such precautions should include:

Do:

- Take appropriate steps to protect office equipment and work-related information from theft and accidental loss or damage.
- Ensure that office equipment (e.g. laptop) and hard copy documents are not left unattended where this might constitute a risk.
- Ensure that casual passers-by or other unauthorised persons cannot read information where this might constitute a risk (e.g. when entering passwords, accessing sensitive personal data).
- Ensure that office equipment and hard copy documents are not accessible to your family or friends.
- Make sure office equipment and hard copy documents left unattended in a parked car are locked away in the boot of the car, out of plain sight.
- Work directly from the Commissioner's office server via a secure network connection.
- Save any electronic documents produced at home on to the Commissioner's office server via the secure network connection.
- Take copies of paper documents home rather than the originals; taking only the minimum of records that you require to work with.
- Return copies of paper documents to the office to ensure that they are disposed of appropriately.
- Familiarise yourself with other relevant policies and guidance (e.g. data protection policy, home working arrangements) in the information handbook.

Do not:

- Download, install or use unauthorised software programs.
- Open an email attachment unless you trust the source.
- Store, use, copy or circulate inappropriate materials (e.g. pornographic, sexually explicit, or racially offensive material) on office equipment (e.g. laptop, mobile phone). If you receive inappropriate material by email or other means delete it immediately and inform the Head of Corporate Services at the earliest opportunity.

- Use your home computer to store work-related information.
- Use a personal email account for work-related business.
- Store confidential or sensitive personal information on a USB memory Stick.
- Store confidential or sensitive personal information on the hard drive of office equipment.

4 Equipment

Staff provided with office equipment to work remotely must only use this for legitimate work-related purposes. The equipment provided may only be modified or replaced by the Commissioner's IT Contractors if authorised by the Head of Corporate Services. Office equipment must be returned at the end of the remote working arrangement.

If staff need to remotely access sensitive personal information as part of their work they must do so using office equipment (e.g. laptop). All office laptops are set-up to enable users to log-in to the Commissioner's office network, where information can be saved onto the server. Staff are responsible for the safekeeping and protection of office equipment issued to them. They are also responsible for preventing unauthorised persons from accessing them.

It is important to note that corporate applications (e.g. TRIM, Filemaker, Sage) are not currently enabled for remote working. Documents that should be saved to these applications will need to be saved to the Commissioner's network in the first instance.

On return to the office equipment must be checked in and signed for by the Head of Corporate Services.

5 Report damage, loss or theft

If office equipment is lost or stolen please notify the Police and the Head of Corporate Services at the earliest opportunity. If you are unable to contact the Head of Corporate Services please notify Dunedin IT of the loss or theft of any office mobile device.

Please report IT security incidents (e.g. virus infections) promptly to the Head of Corporate Services. The damage, loss or theft of any work-related information

while remote working should be reported to the Head of Corporate Services and the Information Officer promptly; where the damage, loss or theft is of sensitive personal information this must be reported immediately to enable a data protection breach to be dealt with appropriately.

6 Right of access to information

The access to information regimes in Scotland; the Data Protection Act 1998, the Freedom of Information (Scotland) Act 2002 and the Environmental Information (Scotland) Regulations 2004 give the general public rights of access to information held by the Commissioner and their office irrespective of media or format. In the event of a request for information staff must retrieve all relevant requested information, whether held on the Commissioner's network or remotely.

7 Policy Review

The Remote Working Policy shall be maintained, reviewed and updated by the Management Team.

Evidence 8.2: Employee Handbook (home working arrangements)

Section 9.2 Annex K: Home Working Arrangements

What is home-working?

Home-working is an arrangement whereby you work from home for all or part of your working day or week on an ad hoc or contractual basis. The Commissioner does not currently offer the option of contractual home working.

Whilst you are working at home, you will continue to be covered by the employment policies of the Commissioner, including the terms and conditions set out within this Handbook and the Data Protection Act 1998.

Home-working is not an alternative to childcare and other care arrangements. You should ensure that you are able to work uninterrupted and not whilst looking after a dependant. This may mean changing your working pattern, e.g. working in the evening when your child is asleep. If your preferred working pattern extends beyond the FWH bandwidth, you should clear any changes you wish to make with your Line Manager.

It is important to note that only certain Microsoft Office applications (Word, Excel, Powerpoint, Outlook) will be available to home workers and corporate applications (e.g. TRIM, Filemaker, Sage etc) are not currently worker enabled.

Ad hoc home-working

There may be particular circumstances where you need to work from home for a short time, on an ad hoc basis, to complete reports, or to work free from distraction. This type of home working will not require a variation to your terms and conditions of service and can be done provided you have the prior approval of your Line Manager.

Where you need to work from home on sensitive personal data you must be authorised to do so by the Head of Corporate Services; an office supplied laptop must be used which is set-up to enable you to securely access the Commissioner's office network. Sensitive personal data consists of information concerning an individual's racial or ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, sexual life and criminal records.

Health and safety for ad-hoc home working

As in the office, you have a responsibility to report all accidents and near misses to the Head of Corporate Services. You also have a responsibility to record all accidents or near misses using an Incident Report form obtainable from the Head of Corporate Services, to whom you should return the completed form.

Security for ad hoc home working

When you are working from home on an ad hoc basis, you will be responsible for the security and safekeeping of work-related records in your care. The 'Remote Working Policy' provides further guidance on the precautions you should take when working from home.

Evidence 8.3: HP TRIM Documentation regarding security administration

TRIM

HP TRIM Software Help > Security > Security administration

Security administration

The security functions in HP TRIM control the user access to records and items held in the dataset.

About security

Put simply, security is protection. It is the desire to prevent harm to something valuable. In the case of HP TRIM, security protects information.

Apart from the obvious need to protect data from deliberate and accidental corruption, theft and destruction, there is also a need to control access to information in a manner that is agreeable to corporate requirements.

The most simplified corporate requirement is to provide a worker with access to relevant data (and controls) to complete tasks.

This suggests that the methods of security must be scalable from complete exclusion to need to know access, privileged access, and full access.

HP TRIM provides a multitude of security options that determine group permission properties.

The options may apply to data objects (records, Locations, etc.), users (logons), class objects (Record Types), and data resources (support and configuration properties).

Caution: Availability of items in HP TRIM depends on the combination of security, Access Controls and permissions that are set both on the item and for the user accessing the item. No security setting will override another security setting. For example, a record may have multiple controls placed upon it to restrict access to it in various ways for different users - security levels, caveats, Access Controls and user type permissions. If the user does not have the same controls, they will not be able to view or modify the item.

Combinations of the security functions ensure that records can be held securely and can only be accessed by users with the permission to view or modify those records.

This control is managed in three ways:

- "Security levels administration"
- "Security caveats administration"
- "Access Control"

See "Applying security and Access Control defaults" - "Copy Style / inheritance" for details about setting defaults and the default **Copy Style** inheritance options.

These are the rules you can apply to control the inheritance of security levels, caveats and Access Controls by objects being created or modified.

Related Topics

Data Protection Policy

Table of Contents

1 Introduction

The Data Protection Act 1998 imposes legal obligations on the processing of personal data held by Scotland's Commissioner for Children and Young People (the Commissioner) and their office (work of the office and/or members of staff). This policy sets out how the Commissioner and the Commissioner's office comply with the Data Protection Act.

This policy and related procedures and guidance aim to ensure the Commissioner and the Commissioner's office fulfils the requirement of fair and lawful processing of personal data in the records created and received in the course of its activities.

This policy complies with the Data Protection Act.

2 Policy Statement

The Commissioner is a data controller, as defined in section 1(1) of the Data Protection Act, and is obliged to ensure that all of the Data Protection Act requirements are implemented. To do this the Commissioner and the Commissioner's office must comply with the eight data protection principles as set out in the Data Protection Act (see Appendix 1).

As part of normal business operations the Commissioner and their office processes personal data about its employees and stakeholders (e.g. service users, suppliers, advisers, journalists). Where required, the Commissioner and their office gives those whose personal data is processed (known as "data subjects") fair notice of the purposes for which their personal data is processed. Processing broadly means obtaining, recording, holding, altering, using, disclosing or disposing of personal data.

The Commissioner and their office ensures that personal data is collected and used fairly, is stored safely, and is managed in accordance with the eight data protection principles by ensuring that personal data is kept secure, accurate, up to date, and disposed of at the appropriate time.

The Commissioner and their office will not disclose personal data to any third party unlawfully.

3 Data subject to the Data Protection Act 1998

The Data Protection Act relates to the processing of personal data. Personal data is data which relates to a living individual who can be identified from the data or from the data combined with other information (not necessarily data), and includes any expression of opinion about the individual. As a public authority, the Data Protection Act applies to all personal data held by the Commissioner and their office, both electronically and manually.

The Data Protection Act categorises some personal data as sensitive personal data. This consists of information concerning an individual's racial or ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health, sexual life and criminal records.

The majority of the personal data held by the Commissioner and their office is not sensitive and is made up of data provided by employees and stakeholders.

4 Right of access to personal data

An individual's right to request their own personal data is known as a subject access request.

Subject access requests are made by the data subject (the individual whose personal data it is) for their personal data held by the Commissioner and their office. In some cases, a subject access request may be made by a third party on behalf of an individual, for example.

- By a parent on behalf of a young child. In Scotland, the law presumes that a child aged 12 years or more has the capacity to make a subject access request.
- By a representative on behalf of an adult with incapacity.
- By a solicitor acting on behalf of a client.

The Commissioner and their office take reasonable steps to make sure that the person making the subject access request is who they say they are. If someone is making a request on behalf of a third party, the Commissioner and their office will check that they have the legal authority to make the request.

The Commissioner's Data Protection Procedures provide full guidance to staff on how to respond to subject access requests.

5 Data Processors

Where the Commissioner and their office uses a contractor to process personal data on its behalf (a "data processor"), the Commissioner and their office must be satisfied that the contractor is taking adequate steps to allow the Commissioner and their office to meet its obligations under the Data Protection Act. Contracts between the Commissioner and data processors must specify the necessary security procedures and other appropriate measures; the contract must be monitored to ensure that it is being adhered to.

6 Governance Arrangements

In order to comply with the Data Protection Act, in addition to this Policy, the Commissioner and their office have business processes and systems which include:

- Identifying a role with specific responsibility for Data Protection.
- The provision and implementation of procedures for the Commissioner's staff on handling personal data.
- Training for all of the Commissioner's staff in data protection and good practice.
- Notification with the Information Commissioner's Office of all uses of personal data within the Commissioner's office.
- An annual report on Information and Records Management to the Management Team.

7 Responsibilities for Data Protection

7.1 All Staff

Every member of staff is required to be aware of the provisions of the Data Protection Act and its impact on the work the Commissioner and the office undertakes. Every member of staff must familiarise themselves with and follow the Commissioner's Data Protection Policy and Procedures. Staff are individually responsible for ensuring that procedures for the collection and use of personal data within their job are complied with.

7.2 Management Team

The Management Team has overall responsibility for the Data Protection Policy. The Management Team is responsible for ensuring the policy and procedures for handling personal data are followed, and that staff competence is maintained and developed. The Head of Corporate Services has direct responsibility for overseeing the work of the Information Officer.

7.3 Information Officer

The Information Officer has responsibility for ensuring that the Commissioner's Data Protection Notification is kept up to date. The Information Officer, in conjunction with the Management Team, reviews and updates the Data Protection Policy and Procedures as necessary. The Information Officer monitors compliance with the Data Protection Policy and Procedures.

Appendix 1 - Data Protection Principles

Schedule 1 of the Data Protection Act lists the Data Protection Principles as:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 2 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Evidence 9.2: Certificate of Registration as a Data Controller

ico.
Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

Certificate of Registration

This is to certify that:

The Commissioner for Children and Young People in Scotland

is registered with the Information Commissioner's Office under registration reference:

Z8626786

Registration Start date:

16 June 2005

Registration Expiry date:

15 June 2016

Evidence 9.3: Employee Handbook (confidentiality and data protection)

8.2.1.1.1 Section 9.2 Annex K Appendix 1: Confidentiality and data protection

The 'Employee Handbook' and the 'Remote Working Policy' provide instructions on the action required in the event that office equipment or sensitive personal information is lost, stolen or damaged. Such events must be reported immediately to the Head of Corporate Services.

When you are working from home, you will be responsible for the security and safekeeping of work-related information in your care. This applies to work-related information held on all electrical equipment including, for example, files and e-mails held on laptops, information held on mobile devices and memory sticks, documents printed in hard copy format and hand written notes. All staff should take the following precautions to protect against the loss or interference with all work-related information.

Do:

- Take appropriate steps to protect office equipment and work-related information from theft and accidental loss or damage.
- Ensure that office equipment (e.g. laptop) and hard copy documents are not left unattended where this might constitute a risk.
- Ensure that office equipment and hard copy documents are not accessible to your family and friends.
- Work directly from the Commissioner's office server via a secure network connection.
- Save any electronic documents produced at home on to the Commissioner's office server via the secure network connection.
- Take copies of paper documents home rather than the originals; taking only the minimum of documents that you require to work with.
- Return copies of paper documents to the office to ensure that they are disposed of appropriately.

Do not:

- Download, install or use unauthorised software programs on office equipment.
- Open an email attachment, unless you were expecting to receive it from the sender.
- Store, use, copy or circulate inappropriate materials (e.g. pornographic, sexually explicit, or racially offensive material) on office equipment (e.g. laptop, mobile phone). If you receive inappropriate material by email or other means delete it immediately and inform the Head of Corporate Services at the earliest opportunity.
- Use your home computer to store work-related information.
- Use a personal email account for work-related business.

- Store confidential or sensitive personal information on a USB memory stick.
- Store confidential or sensitive personal information on the hard drive of portable office equipment (e.g. laptop, mobile phone).

For further advice on data protection issues, please refer to the Data Protection Policy and Procedures in the Information Handbook or contact the Information Officer.

Evidence 9.4: Privacy Notice (Extract from Website)

Privacy and cookies

The purpose of this privacy guide is to tell you what to expect when the Commissioner's office collects **personal information**.

We collect information about:

- visitors to our website
- people who subscribe to our e-newsletter
- people who contact us with a question or a comment for the Commissioner, where we would want to get back in touch to provide them with an answer
- people who want to request a publication or resource from us
- job applicants

Things to know about personal information

- You don't have to provide us with any of your personal details if you don't want to. You are free

What it means

- Someone is **anonymous** when people don't know who they are.
- **CMS** is short for "Content Management System". A Content Management System can be used to create new pages on a website. It can also be used to make changes to pages that are already there.
- **Personal information** is information that can be used to identify a person.
- A **postback** is a type of information exchange. It often

to say "no" at any time.

- If you don't want to provide us with your real name, you might decide to use a nickname instead.
- For your safety, we won't publish your full name or e-mail address on this website.
- We will keep our firewall and security systems up to date to make sure that your details are kept safe at all times.

Keeping your personal information safe

The Data Protection Act 1998 is the law that tells organisations what they must do to keep people's personal details safe and secure.

Organisations have a responsibility to make sure that your private information doesn't fall into the wrong hands or get used in a way that you're not happy with. For example, they should make sure that if you sign up for their newsletter you won't get lots of spam from a different organisation as a result.

Accessing your personal information

If we ever ask you to tell us any of your personal details, we'll tell you:

- why we're asking for it
- what it will be used for

If you're not sure about what this means, please feel

happens when you write something on a website, then click "submit" or "save".

- A **session** is a period of time. On this page, it means the period of time that lasts from when you come to this website until you close your web browser.
- A **web browser** is something that lets you see the internet on a phone, computer or other device. Popular web browsers include Chrome, Internet Explorer and Safari.

free to ask us about this at any time.

You have the right to see any of the information that we holds about you. You can find out more about how to do this by e-mailing us, writing to us or phoning us. If you find that any of the information we've got is wrong, then please tell us and we'll do our best to put it right as soon as possible. There are a very few times when the law says we don't have to provide you with absolutely all the information we have, such as if providing you with that information means that we'd have to reveal personal information about another person. If we can't release all your information, though, we will tell you why.

Sharing your personal information

We will normally only share your info with someone outside the office of Scotland's Commissioner for Children and Young People when we've asked your permission to do this.

However, if we are worried about your safety – or the safety of someone close to you – we might have to pass your information on without your permission. Depending on the circumstances, this might involve us contacting the Children's Reporter, the local social work office or the police. If we did pass on your information, we would normally tell you we were doing so and our reasons why.

1. Business Continuity and Recovery

Depending upon the reason for the disruption the tables below:

- *Set out the critical activities to be recovered, the timescales in which they are to be recovered and the recovery levels needed.*
- *The resources available at different points in time to deliver the critical activities.*
- *The process for mobilising these resources.*
- *Detailed actions and tasks needed to ensure the continuity and recovery of the critical activities.*

They are ordered where information is available in rank order based on the residual risk score

Critical Function 1	
Information	**Details**
Function Title / Description:	**Major Incident** **e.g. fire, flood, fire, wind damage leading to denial of entry to site**
Risk No. on Risk Register	**Risk No.20**
Residual Risk Score **(impact/likelihood)**	**12** - Stakeholder and staff unable to come to organisation. Possible loss of resources and data depending on the incident e.g. fire or flood Building destroyed
Priority:	Having the building safe to get back in to in order to have organisation up and running again Access to and salvage of records – ICT documents are stored on one of three servers. All servers are now fully backed up using the StorageCraft Product suite. Complete images of the server are stored on a local NAS device and every night a mirror of these backup images are uploaded offsite to a private data centre managed in the UK. Salvage of resources and access to speedy replacement of resources
Responsibility:	Head of Corporate Services

Critical Function 1	
Information	**Details**
Recovery Objective and Timescales	
Recovery Time Objective:	**Fully functioning in alternative premises within a week**
Timescales:	1 hour - gather info to decide if BCP needs to be put into action. Is computer network affected? 1 day - office set up at the office of the Commissioner for Ethical Standards in Public Life in Scotland for members of the SMT. 1 day – Following consultation with the IT and phone companies, the Head of Corporate Services will determine how best to provide telephone cover. This may involve redirecting the telephones to an alternative landline or mobile number 1 day - insurance company contacted 1 day - press release issued 1 week - office finder company to find alternative temporary premises
Resources Required for Restoration:	
Staff	All staff need to be aware of situation One or two members of staff who are close to the premises to help salvage any resources, if access to premises allowed Staff who cannot work from the usual office premises will work from home until such time as alternative temporary or permanent accommodation is sourced. All staff have been provided with a copy of this Business Continuity Plan and supplier contact details for use in an emergency. These details should be stored securely at home.
Data / IT / systems	Appropriate back-ups of data. Back up are uploaded off site and maintained by the ICT contractors All staff have remote access, via the internet, to the server, allowing access to all documents and to email. If the circumstances leading to the loss of accommodation also result in the server being inaccessible ,the procedures outlined under “Critical Function 2” will be instituted. Paper data kept as back up for contact numbers on and off organisation premises as an appendix to BCP (See Appendix D)

Critical Function 1	
Information	**Details**
Premises	Alternative premises to be used The office of the Commissioner for Ethical Standards in Public Life in Scotland can offer short term accommodation for the SMT and Communications Manager.
Equipment	Gather salvageable resources from organisation. “Battle box” stored offsite at office of the Commissioner for Ethical Standards in Public Life in Scotland (see Appendix D) for list of content for “Battlebox”)

Critical Function 2	
Information	**Details**
Function Title / Description:	**External break-in/information divulged or lost by SCCYP/IT system and Record Management Plan breached**
Risk No. on Risk Register	**Risk No.3**
Residual Risk Score **(impact/likelihood)**	**10** Loss of confidential/sensitive data and damage to reputation
Priority:	Assess whether Vital Records have been obtained Assess whether Vital Records were protected Recover Vital Records
Responsibility:	Head of Corporate Services
Recovery Objective and Timescales	
Recovery Time Objective:	**ASAP**
Timescales:	1 hour – establish what information has been obtained 1 hour – report to police 1 day – report to insurance company
Resources Required for Restoration:	
Staff	As soon as possible – inform Commissioner, Head of Corporate Services and Information Officer Staff may be asked to work from home until the repair or replacement is completed. In this instance, procedures detailed under "Critical Function 1" (loss of office accommodation) will be followed. The data on the server is regularly backed up. Files can be restored and the backup process is managed by the IT company.
Data / IT / systems **(Business critical applications)**	Installation software for the following packages is held by Dunedin IT TRIM Microsoft Outlook SAGE Filemaker
Premises	Alternative premises may need to be used.

Critical Function 2	
Information	**Details**
Equipment	Gather salvageable resources from organisation. "Battle box" stored offsite at office of the Commissioner for Ethical Standards in Public Life in Scotland (see Appendix D) for list of content for "Battlebox"

Critical Function 3	
Information	**Details**
Function Title / Description:	**Laptops lost or stolen**
Risk No. on Risk Register	**Risk No.2**
Residual Risk Score **(impact/likelihood)**	**9** Loss of confidential/sensitive data and damage to reputation
Priority:	Assess whether Vital Records have been obtained Assess whether Vital Records were protected Attempt to recover laptop
Responsibility:	Head of Corporate Services
Recovery Objective and Timescales	
Recovery Time Objective:	**As soon as possible**
Timescales:	1 hour – establish what records held on laptop and whether member of staff had followed Laptop Security Policy 1 hour – inform police 1 day – inform insurance company
Resources Required for Restoration:	
Staff	As soon as possible – inform Commissioner, Head of Corporate Services and Information Officer
Data / IT / systems	Inform Dunedin IT and remove/disable remote access facility
Premises	n/a
Equipment	Replace laptop and review Laptop Security Policy

Critical Function 4	
Information	**Details**
Function Title / Description:	**Loss of Telephone plus Mobile Telephone communications, IT Crash/Systems Issues**
Priority:	For phone systems to be operational in order to allow administration communication and maintain safety. For IT systems to be operational in order to allow responses to CYP developments
Risk No. on Risk Register	
Residual Risk Score **(impact/likelihood)**	**9** Compromise of data retained Effective Administration and Management affected Stakeholder unable to contact Maintaining stakeholder/staff safety affected ICT systems go down
Recovery Objective and Timescales	
Recovery Time Objective:	ASAP
Timescales:	1 hour - gather info to decide if BCP needs to be put into action. Check if computer network affected. Notify Dunedin IT Support 2 hours – Dunedin IT will escalate and respond 1 day – alternative ways of communicating.
Resources Required for Restoration:	
Staff	Dunedin IT/Commsworld/O2
IT systems	All servers are now fully backed up using the StorageCraft Product suite. Complete images of the server are stored on a local NAS device and every night a mirror of these backup images are uploaded offsite to a private data centre managed in the UK.
Premises	N/A
Equipment	Replace items as necessary

APPENDIX C

Vital Records

What are Vital Records

Vital records are those records that are necessary for the Commissioner's office to continue to operate in the event of disruption or disaster. Examples of disruption include being unable to enter the building for a few hours or days (in the event of, for example, a bomb scare) or being unable to access the Commissioner's office network for a few hours or days; disasters include fire, flood, and the loss of electronic data through malicious electronic intervention. Vital records enable the Commissioner's office to continue functioning in the event of a disaster or disruption, and contain the information needed to re-establish the organisation in the event of a disaster that destroys all other records

Why do we need to bother with identifying vital records

As suggested above, vital records are central to the running of the Commissioner's office. They should be actively identified and steps taken to ensure that the records remain secure and accessible. Identifying vital records forms a part of disaster recovery and business continuity planning, and ensures that the Commissioner's office is well placed to deal with an unexpected event. With limited resources available, the Commissioner's office needs to focus on protecting the right records, it is not worthwhile storing non essential records in the most secure location whilst leaving vital records open to vulnerabilities. Resources need to be targeted at the right records, those that are essential for the Commissioner's office operations, the vital records.

Identifying our vital records

In identifying our vital and non-vital records, these have been classified into several categories as follows:

Classification of records	Description of Record Types
Vital: records without which the Commissioner's office cannot function. These records are essential to the core business of the Commissioner's office (this also includes records which are critical for implementing emergency procedures in the event of a disaster, such as key staff contact details, business continuity plans etc.)	• Records which give evidence of the legal status of the Commissioner • Records which protect the assets and interest of the Commissioner • Minutes and papers of the Senior Management Team • Staff contracts • Current accounts payable and received • The Commissioner's Strategic Plan • The Commissioner's Operational Plan • Research information including on-going research and reports of research projects • Records which are subject to a legal requirement to be kept for a certain amount of time • Historical records if needed for evidential or other legal purposes • Key staff contact details • Next of kin details • Contingency plans
Important: records important to the continued operation of the Commissioner's office, they can be recreated from original sources but only at considerable time and expense.	• Minutes of team meetings
Useful: records which, if lost, would cause temporary inconvenience but are replaceable.	• Most correspondence
Non-essential: records which have no value beyond the immediate purpose.	• Information about specific events that have taken place • recruitment advertisements which are now completed • Newsletters

Protecting Electronic Vital Records

- Electronic vital records are stored on a central server and protected by appropriate back-up and disaster recovery.
- No vital records are stored on portable hardware, such as USBs, DVDs/CDs.
- No vital records are stored on laptop hard drives or personal hard drive.

- Vital records that need to be retained for a long time are saved in a readable format such as PDF, plain text or rich text format. This ensures that they remain accessible even if their original software becomes obsolete.

Protecting Hard Copy Vital Records

Vital records which are only available in paper format are duplicated, in the same or original format depending on requirements, and the originals and copies stored in separate locations.

If duplication is impracticable or legally unacceptable, a fire protection safe is used to protect the documents.

Evidence 11.1: HP TRIM Documentation regarding Audit Trail

TRIM

HP TRIM Software Help > Security > Audit trails

Audit trails

In addition to protecting information from unauthorised access, HP TRIM provides audit trails for authorised access. This ensures you can verify the authenticity of the information.

- Audit logging - monitors and records events that have taken place in the system.
  The HP TRIM Workgroup Server logs events in the audit log. The messaging is guaranteed - when the Workgroup Server is down, the system will queue the messages and the Workgroup Server will process the events when it is back on line.

  The system administrator can define which events are to be logged.
- Active audit events - rather than having to search through the system wide audit log, HP TRIM's active audit event function provides a more convenient method to view the audit trail for one particular record.
  Active audit events lists the events for a record with the following detail:
  - Date and time of the event
  - Logged in user
  - Item affected
  - Type of event
  - Details of the event
  - Whether the event caused a security violation
- Security breaches - in the management of physical records, it is sometimes necessary to allow records to be marked to a Location with a lower security profile than the record itself.
  If this was completely disallowed by HP TRIM - a possible setting - records that physically moved to such a Location could not be tracked in the system. This is why many organisations decide to allow the movement.

  However, every such movement incurs a security breach in HP TRIM. These security breaches are listed in a separate log. A security administrator can then view the breaches that have occurred and investigate them.

Related Topics

Evidence 11.2: HP TRIM Documentation regarding electronic document revisions

TRIM

HP TRIM Software Help > Electronic document management > Electronic document revisions

Electronic document revisions

HP TRIM enables you to create multiple revisions of an electronic document.

A revision is a modified copy of the document. You can attach multiple revisions of an electronic document to a single record.

When you choose to check in an electronic document that has been checked out, you can create a new revision of the document.

A document being returned will be added to the record, the older revision being saved as a previous revision.

Note:

- The last item in the revisions list represents the previous revision, not the current revision. The **Revisions** tab for the selected record in the right-click command **Properties** only appears when a newer version of the document is attached - for example, if you checked out the document, modified it and checked it back in as a new revision. The latest revision is attached to the record, while the previous revisions appear in the **Revisions** tab.
- The **Delete this rendition when cataloguing a new record** option in the HP TRIM Enterprise Studio - **General - File Types - Properties - Renditions** tab deletes the Rendition on the record when you make a new revision. See HP TRIM Enterprise Studio Help about the **Renditions** tab.

This applies to any rendition you mark as such, including digital signatures.

If you do not mark this, the rendition remains.

The new revision will have a digital signature rendition, but it probably will not work because it is the signature associated with the document that has been replaced by the new revision.

Related Topics

Evidence 12.1: Information Officer's Job Description

Job Description

This job description describes the practical purpose and main elements of the job. It is a guide to the nature and main duties of the job as they exist currently, but is not intended as a wholly comprehensive or permanent schedule.

1. JOB DETAILS

Job Title: Information Officer

Department: Corporate Services

Reports to: Head of Corporate Services

Reporting to job-holder: N/A

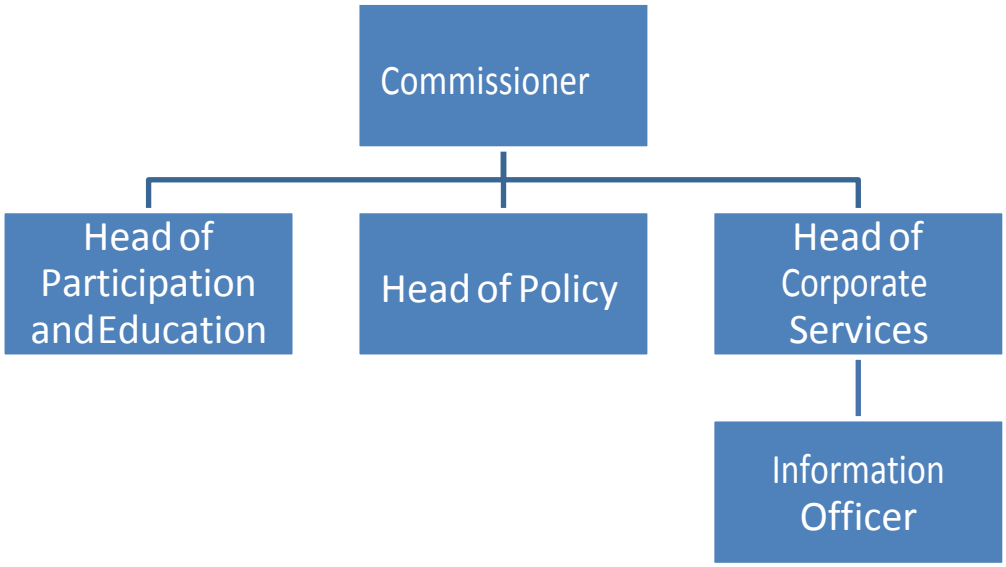
Salary banding: £31,123 - £37,841 (Grade 4)

Last Update: 26/08/2014

2. OVERALL PURPOSE OF THE JOB

To deliver the effective management of information that supports the Commissioner and colleagues in undertaking their work effectively thereby ensuring the promotion and safeguarding of children and young people's rights in Scotland.

3. JOB DIMENSIONS
Structure:



Key Tasks

1. Lead the development and implementation of effective information management governance in accordance with the legislative framework (e.g. Freedom of Information (Scotland) Act, Data Protection Act and Public Records (Scotland) Act) and current best practice.

2. Monitor and collate relevant information in a timely manner to help inform colleagues, particularly with regard to the UNCRC, children's rights and related policy and practice.

3. Develop a knowledge base of information in relation to UNCRC, children's rights and related policy and practice incorporating the provision of papers, journals, books and other external resources for the benefit of colleagues.

4. Undertake desk based research, including literature searches and reviews on behalf of colleagues.

5. Respond to external requests for information in relation to the UNCRC and children's rights.

6. Develop a Children's Rights Impact Assessment process as a means to effective implementation of the UNCRC throughout Scotland.

7. Carry out other similar and appropriate duties as and when required.

Person
Specification

Education	
Essential	Degree educated. Post graduate in information science/management or comparable qualification.
Desirable	Formal training in children's rights or equivalent experience.
Experience	
Essential	Proven experience of managing an information service and/or an information management unit. Proven ability to identify and utilise appropriate external information resources, such as legal and sociological databases. Experience of providing information services to a variety of internal and external audiences using a range of approaches including factsheets, enquiries, desk research, literature searches and reviews, digital media and monitoring. Experience of working in a public/government body and meeting the required standards of public accountability for the management of information and data. Experience of using a range of ICT technology and information management systems in addition to Microsoft office systems.
Desirable	Experience of working in a children's rights environment. Experience of co-ordinating responses to FOI and Subject Access Requests.

Personal Characteristics/Competencies	
Essential	Ability to locate, collate and analyse complex information and data across a wide range of issues sharing information in a timely manner and in an accessible format. The ability to communicate well with a wide range of audiences using the most appropriate method.
Desirable	Commitment to promoting and safeguarding children's rights. Understanding of Scottish political infrastructure and framework. Knowledge of organisations in Scotland working with and for children and young people.

Note:

Every job description will be subject to a review either:

On an annual basis at the time of the annual appraisal meeting,

or as a result of a change in strategic direction, or

as a result of team/operational requirements, or

as a result of agreed performance appraisal needs and

objectives, or within 6 months of appointment

Evidence 12.2: Membership of Information and Records Management Society

irms
the interactive hub of the information world

INVOICE TO:
Scotland's Commission for Children & Young People
Gillian Munro
85 Holyrood Road
Edinburgh EH8 8AU
UNITED KINGDOM

INVOICE DATE: 13/03/2015
INVOICE NO: M4137_2015
MEMBERSHIP NUMBER: 4137
PURCHASE ORDER:
VAT NUMBER:

Description	Net Cost £	VAT £	Total £
Annual Subscription for Corporate Member of IRMS (01 January 2015 to 31 December 2015)			
Portion attributable to the production of the Bulletin	£50.00	£0.00	£50.00
Remaining portion of subscription for Corporate Membership	£250.00	£50.00	£300.00
VAT is only chargeable on that element of the fee which does not apply to the production of the Bulletin			
Total Cost			£300.00
VAT Total			£50.00
GRAND TOTAL			**£350.00**
Payments Received			£350.00
FINAL BALANCE			**£0.00**

Please follow this link to pay for your membership by credit or debit card:
www.irms.org.uk/join/worldpay-renewals

PAYMENT RECEIVED WITH THANKS

IRMS Accreditation - professional accreditation for all information professionals - contact info@irms.org.uk for further details

IRMS • Chester House, 68 Chestergate, Macclesfield, Cheshire, SK11 6DY
Tel: 44 (0) 1625 664520 • Fax: 44 (0) 1625 664510 • info@irms.org.uk • www.irms.org.uk

Evidence 13.1: Operational Plan 2015-2016

AREA OF WORK	OBJECTIVE	ACTIVITY	TIME	LEAD
Information Governance and Records Management	Ensure we comply with FOISA and EISR	Respond to FOI Requests, EISR Requests and requests for review promptly and within statutory timescale. Follow Scottish Information Commissioner good practice when responding to requests. Complete and return quarterly statistics to the Scottish Information Commissioner. Adopt new model publication scheme for FOI.	Ongoing. Respond to FOIs, EIRs and Reviews within 20 working days. New Publication Scheme 31 May 2015.	Information officer
Information Governance and Records Management	Ensure we comply with DPA	Respond to subject access requests and objections to processing of personal data within statutory timescale. Ensure notification in ICO register of data controllers is maintained. Report and mitigate impact of any data protection breaches immediately. Follow ICO good practice guidelines to ensure compliance with DPA.	Ongoing. Respond to SAR's within 40 calendar days. ICO Notification Jun 15.	Information officer
Information Governance and Records Management	Ensure we comply with PRSA	Prepare and implement a Records Management Plan (RMP) that is approved by the Keeper of the Records of Scotland. Improve records management practice within the office by undertaking actions listed under the RMP. The RMP to be reviewed every 6 months.	Ongoing. RMP list of actions (Jun 15 - Mar 16). RMP review Jan 16.	Information officer

Evidence 14.1: Guide to information available through our publication scheme

Guide to information available through the Model Publication Scheme 2015

The Freedom of Information (Scotland) Act 2002 (the Act) requires Scottish public authorities to produce and maintain a publication scheme. Authorities are under a legal obligation to:

- publish the classes of information that they make routinely available
- tell the public how to access the information and what it might cost.

Scotland's Commissioner for Children and Young People has adopted the Model Publication Scheme 2015 produced by the Scottish Information Commissioner. This scheme has the Scottish Information Commissioner's approval until 31 May 2019. You can read this scheme on our website at www.sccyp.org.uk/footer/foi or by contacting us at the address below to request a copy.

The purpose of this Guide to Information is to:

- allow you to see what information is available (and what is not available) in relation to each class;
- state what charges may be applied;
- explain how you can find the information easily;
- provide contact details for enquiries and to get help with accessing the information; and
- explain how to request information we hold that has not been published.

Availability and formats

The information we publish through the model scheme is, wherever possible, available on our website. We offer alternative arrangements for people who do not want to, or cannot, access the information online or by inspection at our premises. For example, we can usually arrange to send information to you in paper copy (although there may be a charge for this).

Exempt information

We will publish the information we hold that falls within the classes of information below. If a document contains information that is exempt under Scotland's freedom of information laws (for example sensitive personal information or a trade secret), we may remove or redact the information before publication but we will explain why.

Copyright

Scotland's Commissioner for Children and Young People has adopted the Open Government Licence for public sector information http://www.nationalarchives.gov.uk/doc/open-government-licence/. This sets out what you can and cannot do with our public information where we are the copyright holder. Where Scotland's Commissioner for Children and Young People does not hold the copyright in information we publish, we will make this clear in this guide.

Charges

This section explains when we may make a charge for our publications and how any charge will be calculated. There is no charge to view information on our website or at our premises.

We may charge for providing published information to you e.g., photocopying and postage, but we will charge you no more than it actually costs us to do so. We will always tell you what the cost is before providing the information to you.

Our charges are as follows:

- Photocopying at 5p per black and white A4 sheet and 10p per colour A4 sheet.
- Information provided on CD-Rom will be charged at £0.50 per computer disc.
- We will recharge any postage costs at the rate we paid to send the information to you.
- When providing copies of pre-printed publications, we will charge no more than the cost per copy of the total print run.

We do not pass on any other costs to you in relation to our published information.

Requesting information which is not in our publication scheme

If the information you want is not in our publication scheme, you have the right to request it from us. The Freedom of Information (Scotland) Act 2002 gives you a right of access to the information we hold (whether we publish it or not), subject to certain exemptions. You do not have to tell us why you want the information or what you plan to do with it. Requests can be made at the address below.

We may charge for unpublished information provided in response to a request for it. Where it would cost us £100 or less to provide the information to you, we will not impose a charge. Where information costs between £100 and £600 to provide to you, we may ask you to pay 10% of that part of the cost. Where it would cost more than £600 to provide information to you, we may ask you to pay the costs as set out above up to £600, and the remaining costs over £600 in full.

Contact us

You can contact us for assistance with any aspect of this publication scheme:

Scotland's Commissioner for Children and Young People
9 Haymarket Terrace
Edinburgh
EH12 5EZ

Telephone:	0131 346 5350
Fax:	0131 337 1275
Email:	info@sccyp.org.uk

We will also advise you how to ask for information that we do not publish or how to complain if you are dissatisfied with any aspect of this publication scheme.

The classes of information that we publish

We publish information that we hold within the following eight classes. Once information is published under a class we will continue to make it available for the current and previous two financial years.

Where information has been updated or superseded, only the current version will be available. If you would like to see previous versions, you are may make a request to us for that information.

Class 1: About Scotland's Commissioner for Children and Young People
Class description: Information about the Commissioner and his office, who we are, where to find us, how to contact us, how we are managed and our external relations.

The information we publish under this class	**How to access it**
Law establishing us	
Commissioner for Children and Young People (Scotland) Act 2003	http://www.legislation.gov.uk/asp/2003/17/contents
Children and Young People (Scotland) Act 2014, Part 2	http://www.legislation.gov.uk/asp/2014/8/contents
About us	
Commissioner's role	http://www.sccyp.org.uk/about/commissioner/role
Commissioner's team	http://www.sccyp.org.uk/about/team
History of the Commissioner	http://www.sccyp.org.uk/about/history
Contacting us	
Contact us	http://www.sccyp.org.uk/footer/address

Complain about us	http://www.sccyp.org.uk/ufiles/Complaints-Procedure.pdf
Accessibility	http://www.sccyp.org.uk/footer/accessibility
Governance and accountability	
Advisory Audit Board	http://www.sccyp.org.uk/footer/foi/class-4/advisory-audit-board
Managing the organisation	http://www.sccyp.org.uk/footer/foi/class-3/management
Risk management policy	http://www.sccyp.org.uk/ufiles/Risk-Management-Policy.pdf
Scheme of delegation	http://www.sccyp.org.uk/ufiles/Scheme-of-Delegation-2015.pdf
Keeping others informed	
Newsletter	http://www.sccyp.org.uk/news/newsletter
Press releases	http://www.sccyp.org.uk/news/pressreleases
Speeches and presentations	http://www.sccyp.org.uk/about/speeches
Commissioner's Facebook page	https://www.facebook.com/RightsSCCYP
Commissioner on Twitter	https://twitter.com/rightssccyp
Commissioner's You Tube channel	https://www.youtube.com/user/RightsSCCYP

Class 2: How we deliver our functions and services
Class description: Information about our work, our strategy and policies for delivering functions and services and information for our service users.

The information we publish under this class	How to access it
Workplans and annual reporting	
Annual accounts and reports	http://www.sccyp.org.uk/about/annual
Strategic plan	http://www.sccyp.org.uk/footer/foi/class-2/strategic-plan
Operational plan	Not currently available on website – please contact us for a hard copy
Equality duty and outcomes	http://www.sccyp.org.uk/footer/foi/class-2/equality
Corporate parenting plan	Not currently available on website – please contact us for a hard copy
Review of law, policy and practice of children's rights	
Child rights monitoring	http://www.sccyp.org.uk/policy/child-rights-monitoring
Child rights impact assessment	http://www.sccyp.org.uk/policy/cria
Consultation responses	http://www.sccyp.org.uk/policy/evidence
Parliamentary evidence	http://www.sccyp.org.uk/policy/evidence
Policy briefings	http://www.sccyp.org.uk/policy/briefings
Publications	http://www.sccyp.org.uk/publications
Research	http://www.sccyp.org.uk/policy/research
Promoting awareness and understanding of children's rights	
Rights resources (instructional workshops and activities)	http://www.sccyp.org.uk/education/rights-resources
Golden rules for	http://www.sccyp.org.uk/education/golden-rules

participation	
Current work	http://www.sccyp.org.uk/education/current-work
Past work	http://www.sccyp.org.uk/education/past-work
Rights in pictures (illustrated guide to the UNCRC)	http://www.sccyp.org.uk/education/rights-in-pictures

Class 3: How we take decisions and what we have decided
Class description: Information about the decisions we take, how we make decisions and how we involve others.

The information we publish under this class	**How to access it**
Managing the organisation (includes Management Team minutes)	http://www.sccyp.org.uk/footer/foi/class-3/management
Scheme of delegation	http://www.sccyp.org.uk/ufiles/Scheme-of-Delegation-2015.pdf
Advisory Audit Board	http://www.sccyp.org.uk/footer/foi/class-4/advisory-audit-board
Consultation with children and young people	http://www.sccyp.org.uk/education/past-work/blether http://www.sccyp.org.uk/education/past-work/wee-blether
Consultation with organisations	http://www.sccyp.org.uk/downloads/SCCYP_Strategic_Plan_12-16.pdf

Class 4: What we spend and how we spend it
Class description: Information about our strategy for, and management of, financial resources (in sufficient detail to explain how we plan to spend public money and what has actually been spent.

The information we publish under this class	**How to access it**
Budget and expenditure	
Annual accounts	http://www.sccyp.org.uk/about/annual
Annual statement of expenditure	http://www.sccyp.org.uk/footer/foi/class-4/annual-expenditure
Commissioner's expenses (in monthly expenditure reports)	http://www.sccyp.org.uk/footer/foi/class-4/budget-expenditure
Monthly expenditure	http://www.sccyp.org.uk/footer/foi/class-4/budget-expenditure
Financial accountability	
Advisory Audit Board	http://www.sccyp.org.uk/footer/foi/class-4/advisory-audit-board
Annual audit reports	http://www.sccyp.org.uk/footer/foi/class-4/advisory-audit-board
Financial accountability	http://www.sccyp.org.uk/footer/foi/class-4/financial-accountability
Financial memorandum	http://www.sccyp.org.uk/ufiles/Financial-Memorandum-Manual.pdf
Contracts and procurement	
Procurement policy	http://www.sccyp.org.uk/ufiles/Procurement-Policy.pdf

Value of contracts	http://www.sccyp.org.uk/ufiles/Standing-Contracts-2014-2015.pdf

Class 5: How we manage our human, physical and information resources
Class description: Information about how we manage the human, physical and information resources of the Commissioner's office.

The information we publish under this class	**How to access it**
Office policies	
Anti fraud policy	http://www.sccyp.org.uk/ufiles/Anti-Fraud-Policy.pdf
Child protection procedures	http://www.sccyp.org.uk/ufiles/Child-Protection-Procedures.pdf
Complaints procedure	http://www.sccyp.org.uk/ufiles/Complaints-Procedure.pdf
Personal use of social media	http://www.sccyp.org.uk/ufiles/Personal-use-of-Social-Media.pdf
Professional use of social media	http://www.sccyp.org.uk/ufiles/Professional-use-of-social-media.pdf
Managing information	
Data protection policy	http://www.sccyp.org.uk/ufiles/data-protection-policy.pdf
Freedom of information policy	http://www.sccyp.org.uk/ufiles/FOI-Policy.pdf
Information and records management policy	http://www.sccyp.org.uk/ufiles/Information-and-Records-Management-Policy.pdf

Model publication scheme and guide to information	http://www.sccyp.org.uk/footer/foi/guide
Remote working policy	http://www.sccyp.org.uk/ufiles/Remote-Working-Policy.pdf
Managing employees	
Employee handbook	http://www.sccyp.org.uk/ufiles/Employee-Handbook.pdf
Recruitment and selection policy (in the employee handbook)	http://www.sccyp.org.uk/ufiles/Employee-Handbook.pdf
Employee survey	http://www.sccyp.org.uk/ufiles/Employee-Survey.pdf

Class 6: How we procure goods and services from external providers
Class description: Information about how we procure goods and services, and our contracts with external providers.

The information we publish under this class	**How to access it**
Current invitations to tender	http://www.sccyp.org.uk/footer/foi/class-4/contracts-and-procurement
Procurement policy	http://www.sccyp.org.uk/ufiles/Procurement-Policy.pdf
Value of contracts let by the Commissioner	http://www.sccyp.org.uk/ufiles/Standing-Contracts-2014-2015.pdf

Class 7: How we are performing

Class description:
Information about how the Commissioner's office performs as an organisation, and how well it delivers its functions and services.

The information we publish under this class	**How to access it**
Advisory Audit Board	http://www.sccyp.org.uk/footer/foi/class-4/advisory-audit-board
Annual accounts	http://www.sccyp.org.uk/about/annual
Annual audit reports	http://www.sccyp.org.uk/footer/foi/class-4/advisory-audit-board
Annual reports	http://www.sccyp.org.uk/about/annual
External evaluations	http://www.sccyp.org.uk/footer/foi/class-7

Class 8: Our commercial publications
Class description:
Information packaged and made available for sale on a commercial basis and sold at market value through a retail outlet e.g. bookshop, museum or research journal.

The information we publish under this class	**How to access it**
We do not hold or publish any information under this class.	

Appendix 4 – Document Control

Document Information				
Document name	Records Management Plan			
TRIM No.	DOC/15/675			
Type	Policy			
Prepared by	Information Officer			
Date	24/04/2015			
Approval				
Approved by	Management Team			
Approval Date	27/04/2015			
For publication (Y/N)	Yes			
Review				
Responsible Manager	Head of Corporate Services			
Date of next review	01/01/2016			
Publication				
Date published on website				
Summary of changes to document				
Date	Action by *(initials)*	Version updated *(e.g. v1)*	New version no. *(e.g. v2)*	Brief description *(e.g. updated section 1, corrected typos, reformatted)*
18/08/2015	GM	V1	V2	Changes to all elements except 1,2 and 8. Evidence 3.1, 9.2, 10.1, 14.1 replaced by updated versions. Evidence 6.5, 6.6, and 7.1 added. Appendix 1 amended.