Records Management Policy and Retention Schedules

Contents

1. Policy 2
   1.1 Records Management 2
   1.2 Introduction 3
   1.3 What does this policy apply to? 3
   1.4 Who does this policy apply to? 3
   1.5 Why do we need to manage records? 4
   1.6 Records management and knowledge management 4
   1.7 Regulatory Environment 5
2. Roles and Responsibilities 5
   2.1 Introduction 5
   2.2 Specific responsibilities 5
      2.2.1 Head of Corporate Services 5
      2.2.2 Heads of Service 6
      2.2.3 Responsibilities of the Records Manager 6
      2.2.4 The Role of Managers 6
      2.2.5 All staff 7
3. Standards 7
   3.1 What are records? 7
      3.1.1 authentic 7
      3.1.2 reliable 8
      3.1.3 integrity 8
      3.1.4 useable 8
   3.2 How do I decide what is a record? 8
   3.3 Version control 8
   3.4 Capturing and registering records in Objective 8
   3.5 How long do we need to keep our records? 9
   3.6 OSCR vital records 9
   3.7 Subject classification and indexing 9
   3.8 Protective markings 10
   3.9 Understanding Terminology 10
   3.10 Storing and handling records 10
   3.11 Access and security of stored records 11
   3.12 Transferring records to the National Archives of Scotland 11
   3.13 When and how do we dispose of records? 12
Annex A: Glossary of terms 13
Annex B: References and Links 16
Annex C: HM Government Protective Markings 18
Annex D: OSCR Retention Schedules 21

Version Control

Version Number	1
Date signed off (SMT)	
Next Review	August 2010

1. Policy

Accurate and relevant information is vital to the efficient running and management of the Office of the Scottish Charity Regulator (OSCR). We need to balance:

- our statutory obligations (for example, providing the public with information on charities through the Register); with
- our desire to be open and transparent (OSCR's Vision and Values); and
- our duties of confidentiality for personal and sensitive records.

OSCR will comply with all relevant legislation and aims to achieve standards of best practice in records management by adopting principles from such bodies as the British Standards Institute (BSI) and the International Organisation for Standardisation (ISO).

We will ensure that staff have access to records management training and will encourage staff to manage records properly by providing supporting standards, procedures and guidelines.

1.1 Records Management

The principle of records management is to ensure that a record is managed through its full life cycle: from creation through to final disposal.

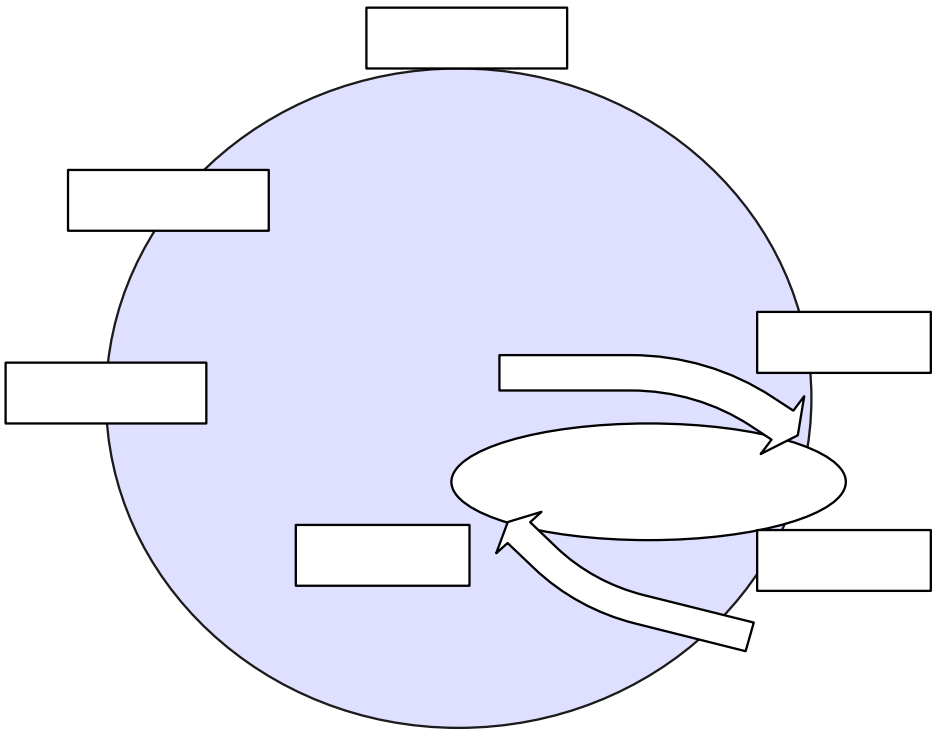

Diagram adapted from BS ISO 15489-1

1.2 Introduction

OSCR is required by law to manage our records properly; legislation such as the Data Protection Act 1998 (DPA) and the Freedom of Information (Scotland) Act 2002 (FOISA) are particularly relevant as they set out specific requirements on the creation and management of records.

A full list of all relevant Acts can be found in this policy under 1.7 Regulatory Environment.

This policy aims to make sure that all OSCR staff understand what they must do to protect and manage records effectively. Each team is responsible for developing working procedures for the day-to-day management of their records. This policy is based on the international standard for records management ISO 15489 and is also supported by a set of records management standards, which include:

- OSCR's document naming conventions;
- E-mail management policies;
- OSCR Information Management principles;
- Version control policy; and
- Information security policy.

1.3 What does this policy apply to?

This policy applies to the management of all records, in all physical forms or media, created or received by OSCR while carrying out its business activities.

Examples of types of record include:

- documents (including written, typed or annotated copies);
- paper files;
- photographs;
- electronic files (including word-processed documents, databases, spreadsheets and presentations) including on disks or CDs;
- e-mail messages;
- brochures and reports;
- annual Monitoring Forms including accounts;
- HMRC Charity Title Files;
- internet pages; and
- faxes.

1.4 Who does this policy apply to?

This policy and any standards associated with it apply to anyone who has access to OSCR records, in whatever form and can include:

- permanent staff members;
- temporary staff members;
- contractors;
- consultants;

- secondees.

1.5 Why do we need to manage records?

Effective records management helps us to meet our statutory obligations and responsibilities as a regulator by:

- helping us carry out our business;
- making sure we comply with relevant legislation;
- supporting the development of evidence-based policy making;
- helping us make informed decisions;
- keeping track of policy changes;
- ensuring that we identify legal precedents;
- supporting consistency in management and administration;
- protecting the rights of employees, charities and the general public;
- providing an audit trail to meet business, regulatory and legal requirements;
- making sure that we work effectively as a regulator and prosecuting authority and meet our lawful obligations for disclosing evidence;
- promoting our activities and achievements;
- making sure we are open and transparent as set out in our Vision and Values.

1.6 Records management and knowledge management

OSCR's records are a form of corporate memory store in which we can accumulate knowledge about our operations as regulator and Scottish Charities over time. When records are properly managed, they can be mined as a rich source of information. Over time, these records will help provide information about trends, whether about processes, transactions or people.

Records can become the raw material and building blocks of knowledge within an organisation such as OSCR, as illustrated in the table below:

Record type	**Knowledge management category**
Charity Correspondence	Types of complaint, knowledge of charity trends, future trends
Case files	Knowledge useful for assessing patterns of compliance
Policy files	Research and development of policy, process improvement
Management plans and papers	Governance and compliance

There is clearly a relationship between records management and knowledge management. Although good records management does not ensure or guarantee OSCR any form of knowledge management capability, the absence of good corporate standards in records management will make any form of knowledge management impossible.

1.7 Regulatory Environment

This policy complies with the following acts, regulations and best practice standards:

- Freedom of Information (Scotland) Act, 2002
- Code of Practice on Records Management published under S.61 of the Act
- Environmental Information (Scotland) Regulations, 2004
- Data Protection Act, 1998
- Human Rights Act, 1998
- Electronic Communications Act, 2000
- International Standard on Records Management, BS ISO 15489
- Principles for Good Practice for Information Management, PD0010: 1997
- In partial compliance with PD0008 Legal admissibility and evidential weight of information stored electronically

2. Roles and Responsibilities

2.1 Introduction

OSCR owns all records that are created by its employees carrying out activities on behalf of OSCR. Individual employees do not own records but they do have responsibilities for managing records. This policy document sets out their roles and responsibilities for managing records.

2.2 Specific responsibilities

SMT collectively, headed by the Chief Executive as Accountable Officer, have overall responsibility for OSCR's records management policy and standards and for supporting their application throughout the organisation

2.2.1 Head of Corporate Services

The Head of Corporate Services has responsibility for the development and implementation of OSCR records management including:

- Ensuring the development of RM policy, standards and corporate procedures
- Ensuring the architecture for systematic implementation of policy, standards and procedures
- Ensuring the identification of corporate resource requirements including internal customer service support
- Decisions on storage of OSCR records

In operational terms much of this is delegated to the Quality Assurance Knowledge Manager (QAKM) but the Head of Corporate Services has key accountability for systems architecture and support.

2.2.2 Heads of Service

OSCR's four Heads of Service have responsibility for making sure that records within their team are managed in accordance with the RM policy including:

- Operating records management procedures covering both electronic and hard copy records that comply with this policy and Information management Principles
- Ensuring the development and operation of quality assurance to cover records management and principles
- Ensuring that they identify and allocate sufficient resources to this responsibility
- Co-operating with other staff, particularly the QAKM and other Heads of Serve to design and operate any tailored procedures not devised on an OSCR wide basis

In operational terms much of this may be delegated to Business Managers but the Heads of Service have key accountability for systems operation

2.2.3 Responsibilities of the Records Manager

The QAKM has operational responsibility for records management, including:

- Ensuring that the RM policy and standards are up to date
- Development of corporate OSCR wide procedures (such as naming conventions , version control, protective markings, disposal inc transfer of records to National Archives Scotland)
- Supporting the Heads of Service to develop and adjust appropriate tailored procedures to comply with RM policy and standards and be compatible with other OSCR procedures
- Undertaking specific RM tasks especially disposal and assisting the Head of Resource decisions on storage
- Monitoring the implementation of RM policy, standards and procedures and providing feedback to the Heads of Service and Chief Executive

Providing internal customer service support including structured communication of RM policy, standards and procedures and giving advice and guidance where required

2.2.4 The Role of Managers

Managers at all levels are responsible for:

- developing and operating records management procedures, covering both electronic and hard copy records that comply with this policy and standards;

- making sure that sufficient team resources are dedicated to the above;

- quality assurance of team records management processes and practices.

2.2.5 All staff

All staff are responsible for:

- Familiarising themselves with OSCR's RM policy and Information management principles
- Following OSCR RM procedures
- Providing constructive input and feedback to allow the continuous improvement of systems and procedures

3. Standards

3.1 What are records?

ISO 15489 describes records as "information created, received and maintained as evidence and/or information by an organisation or person, in pursuance of legal obligations or in the transaction of business."

Documents or e-mails that might constitute a record are likely to contain:

- information relating to business transactions that have or are going to take place
- decisions taken in relation to the business transaction or any discussion that took place in relation to the transaction. For example, during the decision to put out a tender document for a particular service, background discussion about what this should and should not include might take place via e-mail and should be captured as a record.

A record, therefore, should correctly reflect what was communicated or decided or the action that was taken. It should also be able to support OSCR's business needs and can be used for accountability purposes.

Records Management procedures and practices must result in records that have the following characteristics:

3.1.1 authentic

An **authentic** record is one that OSCR can prove to:

- be what it claims to be
- have been created or sent by the person said to have created or sent it
- have been created or sent at the time claimed
- have not been tampered with
- be credible and can be relied on as evidence before an appeals panel or the Courts

To ensure the authenticity of OSCR's records, there are documented procedures that control the creation, receipt, transmission, maintenance and disposition of records.

3.1.2 reliable

A **reliable** record is one whose contents can be trusted, as a full and accurate representation of OSCR's business transactions or activities. This means that OSCR staff should create records within the EDRM system at the time of the transaction or activity to which they relate. Records should be created by OSCR staff with direct knowledge of the facts.

3.1.3 integrity

The **integrity** of a record refers to it being complete and unaltered. Records should be protected against unauthorised alteration. Teams should ensure that records management procedures specify what additions or changes can be made to a record after it is created. Any authorised annotation, addition or deletion to a record should be traceable. The QAK Manager will hold meetings with each team to discuss records management procedures and integrity in respect of that team.

3.1.4 useable

A **useable** record is one that can be located, retrieved, presented and interpreted. This means that we can present that record as being directly connected to the business activity or transaction that produced it. The use of OSCR's Business Classification Scheme and Naming Conventions will help ensure this.

3.2 How do I decide what is a record?

To decide whether something is a record, we should look in the context of:

- OSCR's statutory functions;
- business or accountability requirements; and
- the risk of not keeping it.

3.3 Version control

When we develop policy, it is common to produce successive drafts of a document. These can provide useful evidence of substantial changes during the development of that policy but need to be managed carefully.

OSCR's EDRM system, Objective, supports version control and this is supported by guidance and procedures for staff.

3.4 Capturing and registering records in Objective

Capturing a record means putting the record in a records management system. OSCR uses Objective and to a lesser degree, Logica, for this purpose.

We need to capture items (documents, e-mails, correspondence) to:

- establish a relationship between the record, the staff member who created it and the reason why that records was created;
- place the record and its relationship within a record system;
- link it to other (related) records;
- ensure that appropriate audit trails are maintained.

When capturing records, we need to fill in metadata - such as the charity number or name of the organisation. This is essential to show its relationship with other records. Objective will then register that record with a unique identifier within the system. Registration formalises the capture of the record within the system.

3.5 How long do we need to keep our records?

OSCR has produced a business classification scheme and retention schedules which set out the categories of records we keep and how long we keep those records. OSCR's records retention schedule is attached as Annex D. We review and assess - at least annually - both the retention schedule and business classification scheme against:

- the statutory and regulatory environment
- business and accountability requirements
- the Risks associated with keeping or disposing of a record at any particular point in time

The QA/ Knowledge Manager is responsible for disposing of records in line with OSCR's retention schedule.

3.6 OSCR vital records

OSCR maintains a small number of vital records which have been identified to ensure business continuity in the event of a disaster. These records are kept securely off-site. Further information is available from OSCR's Disaster Recovery Plan.

3.7 Subject classification and indexing

OSCR makes use of a subject classification scheme to classify records. This is based on functions and business activities and helps us to manage our records effectively, by:

- providing links between individual records we collect for a continuous record of activity;
- making sure records are named consistently over time;
- helping to retrieve all records about a particular function or activity;

- deciding security protection for the management of particular sets of records;
- allocating user permissions for access to sets of records; and
- deciding appropriate retention periods and disposition actions for records

In addition, our records management system, Objective, indexes all the records held in the electronic record store. These indices allow us to:

- Search easily for metadata associated with records (file numbers, document names etc)
- Search the content of certain documents (full text indexing)

3.8 Protective markings

OSCR staff must exercise caution and a duty of care when taking copies of documents out of the office. Staff must consider the need for protective markings and this is of particular relevance for:

- Key policy documents or drafts
- Documents relating to inquiries into misconduct or mismanagement

OSCR makes use of the UK Government system of protective markings for this purpose. OSCR will only rarely handle documents with a restricted or protect marking. See Annex C

3.9 Understanding Terminology

It is important that all staff have an understanding of the terms commonly used in respect of Records Management. For this reason, staff should familiarise themselves with the glossary included as Annex A of this document.

3.10 Storing and handling records

As an organisation, we need to consider the specific physical properties of records to decide how to store and handle them. Records that continue to be useful and relevant, no matter what format they are in, need appropriate storage and handling to preserve them for as long as they are needed.

Storage conditions and handling processes should be designed to protect records from unauthorised access, loss or destruction, and from theft and disaster.

Records should be stored on media that ensure their usability, reliability, authenticity and preservation for as long as they are needed. Issues relating to the maintenance, handling and storage of records arise throughout their existence.

Systems for electronic records should be designed so that records are accessible, authentic, reliable and useable through any kind of system

change, for as long as they are kept. This may include transfer to different software, formats or any other future ways of re-presenting records. Where such processes occur, evidence of these should be kept, along with details of any variation in records design and format.

3.11 Access and security of stored records

The regulatory environment in which we operate sets the broad principles on access rights, conditions and restrictions that should be incorporated into the design of our records systems. We have also considered the impact of legislation covering areas such as privacy, data protection, freedom of information and security.

OSCR's records may contain personal, commercial or operationally sensitive material. And in some cases access to the records may be restricted. OSCR carefully considers the use and application of any restrictions, in the knowledge that requests for information under FOISA or the DPA may require the release of information, regardless of any internal access restrictions applied.

Managing the access process involves ensuring that:

- records processes and transactions are only undertaken by those authorised to perform them; and
- parts of the organisation with responsibility for particular business functions specify access permissions relating to their area of responsibility.

Monitoring and mapping of user permissions and functional job responsibilities is a continuing process and the responsibility of the QA/ Knowledge Manager.

All OSCR staff must understand:

- their responsibilities for compliance with information security procedures;
- that OSCR records are unrestricted unless access restrictions have been explicitly requested and put in place;
- the process for having restrictions added or removed;
- their responsibilities under the Data Protection Act for handling records about named individuals;
- how to protect records using security markings.

3.12 Transferring records to the National Archives of Scotland

OSCR will work with the National Archives of Scotland to identify and select records for permanent preservation. These will be records that show the significance of the functions and activities of OSCR in respect of:

- The history of OSCR, its organisation, policies and achievements

- The implementation, enforcement and interpretation of the Charities and Trustee Investment (Scotland) Act 2005.

3.13 When and how do we dispose of records?

The process of disposition - deciding whether to keep, move or destroy records - is governed by OSCR's retention schedules. How long we keep our record is based on guidance from the National Archives on best practice or where that is not available, discussion and agreement with the business area. Case work falls into this latter category and a consistent approach has been applied across the organisation.

Disposition is the:

- immediate physical destruction, including overwriting and deletion;
- retention for a further period within the business unit;
- transfer to an appropriate storage area; or
- transfer of records to an external archive, for example, the National Archives of Scotland.

OSCR has produced retention schedules (See Annex D) that clearly state the retention period of each type of record we capture. Records are reviewed on a monthly basis to identify which records are due for disposal.

Only the QA/ Knowledge Manager is authorised to destroy records in line with OSCR's record retention schedules. A record should be held of which items have been destroyed.

Annex A: Glossary of terms

Access

Right, opportunity, means of finding, using or retrieving information. [ISO 15489]

Accountability

Principle that individuals, organisations, and the community are responsible for their actions and may be required to explain them to others. [ISO 15489]

Accounting Officer (Information Risk)

The Accounting Officer (OSCR's CEO) has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

Capture

Putting a record in a records management system.

Classification

Systematic identification and arrangement of business activities and/or records into categories according to structured conventions, methods, and procedural rules represented in a classification system. [ISO 15489]

Destruction

Process of eliminating or deleting records, beyond any possible reconstruction. [ISO 15489]

Disposition (keeping, moving or removing records)

Range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments. [ISO 15489]

Document

Recorded information or object which can be treated as a unit. [ISO 15489]

Indexing

Process of establishing access points to facilitate retrieval of records and/or information. [ISO 15489]

EDRM

Electronic Records and Document Management System

Information Asset Owner (Information Risk)

Information asset owners are senior individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide written input to the SIRO annually on the security and use of their asset. Within OSCR, IAOs may include the relevant business managers from each team.

Metadata

Data describing context, content and structure of records and their management through time.

Objective

The brand name for OSCR's EDRM system

Permissions

A set of access rules within Objective that define which people or groups can access which records or classes of record.

Preservation

Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time. [ISO 15489]

Records

Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. [ISO 15489]

Records Management

Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. [ISO 15489]

Registration

Act of giving a record a unique identifier on its entry into a system [ISO 15489]

Retention Schedule

See disposition.

Protective Marking

A system of protective markings used in Central Government for documents to restrict access.

Senior Information Risk Officer (Information Risk)

The Senior Information Risk Officer is an executive familiar with information risks and leads the Department's response. The SIRO is the focus for the management of information risk at Board level.

Vital records

Records that are essential to the continued operation of OSCR in the event of a disaster (Disaster Recovery)

Annex B: References and Links

International Organization for Standardization (ISO). *Information and Documentation Records management.* ISO 15489 2000

International Organization for Standardization (ISO). *Information and Documentation - Documentation storage requirements for archive and library materials*. ISO/IEC DIS 11799

The National Archives. Guidelines on developing a policy for managing email. 2004

The National Archives. Guidelines on developing a Records Management policy

The National Archives. Guidelines on Disposal Scheduling

The National Archives. Business Classification Scheme design

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 2. Employee Personnel Records

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 3. Accounting Records

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 4. Health and Safety Records

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 5. Contractual Records

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 6. Project Records

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 8. Press and Public Relations Records

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 9. Press and Public Relations Records

The National Archives – Records Management Advice, Retention and Disposal schedules – Retention Scheduling 11. Internal Audit Records

Scottish Executive Records Management Manual (2005 edition)

Freedom of Information (Scotland) Act, 2002

Code of Practice on Records Management published under S.61 of the Freedom of Information (Scotland) Act

Environmental Information (Scotland) Regulations, 2004

Data Protection Act, 1998

Human Rights Act, 1998

Electronic Communications Act, 2000

Annex C: HM Government Protective Markings

The Protective Marking to be applied to any asset, including information, will be determined primarily by reference to the practical consequences that are likely to result from the deliberate compromise of that asset or information.

The marks determine the level of protection required and are:

Top Secret

The compromise of this information or material would be likely to:

- threaten directly the internal stability of the UK or friendly countries;
- lead directly to widespread loss of life;
- cause exceptionally grave damage to the effectiveness of security of the UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations;
- cause exceptionally grave damage to relations with friendly Governments; or
- cause severe long-term damage to the UK economy.

Secret

The compromise of this information or material would be likely to:

- raise international tension;
- damage seriously relations with friendly Governments;
- threaten life directly or prejudice seriously public order or individual security or liberty;
- cause serious damage to the operational effectiveness or security of the UK or allied forces or to the continuing effectiveness of highly valuable security or intelligence operations; or
- cause substantial material damage to national finances or economic and commercial interests.

Confidential

The compromise of this information or material would be likely to:

- materially damage diplomatic relations, i.e. cause formal protest or other sanction;
- prejudice individual security or liberty;
- cause damage to the operational effectiveness or security of the UK or allied forces or to the effectiveness of valuable security or intelligence operations;
- work substantially against national finances or economic and commercial interests;
- substantially to undermine the financial viability of major organisations;
- impede the investigation or facilitate the commission of serious crime; or

- shut down or otherwise substantially disrupt significant national operations.

Restricted

The compromise of this information or material would be likely to:

- affect diplomatic relations adversely;
- make it more difficult to maintain the operational effectiveness or security of the UK or allied forces;
- cause financial loss or loss of earnings potential to or facilitate improper gain or advantage for individuals or companies;
- prejudice the investigation or facilitate the commission of crime;
- impede the effective development or operations of Government policies;
- disadvantage Government in commercial or policy negotiations with others; or
- undermine the proper management of the public sector and its operations.

Protect*

The compromise of this information or material would be likely to:

- cause substantial distress to individuals;
- breach proper undertakings to maintain the confidence of information provided by third parties;
- breach statutory restrictions on the disclosure of information;
- cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies;
- prejudice the investigation or facilitate the commission of crime; or
- disadvantage Government in commercial or policy negotiations with others.

(*PROTECT is not a national security classification unlike TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED. It has been introduced to cover official information which needs to be protected from compromise of confidentiality, integrity and availability to a known level of assurance, but for which the measures required to safeguard national security information at RESTRICTED are considered disproportionate. To ensure PROTECT is correctly applied across a very wide range of material, it should be accompanied by a **'descriptor'**.)

Descriptors

The following Descriptors to be used with a Protective Mark, where appropriate, reinforce the 'need to know' principle by indicating the nature of the sensitivity involved and limit access accordingly. Descriptors should not be used without a Protective Mark, except for the Descriptor 'Personal'.

- Advice to Ministers - when consulting Ministers on a decision on the development of a new or existing policy or sensitive issue.

- Appointments - concerning actual or potential appointments that have not yet been announced.
- Budget - concerning proposed or actual measures for the Budget before its announcement.
- Commercial - relating to a commercial undertaking's processes or affairs.
- Contracts - concerning tenders under consideration and the terms of tenders accepted.
- Honours - concerning the actual or potential award of an Honour before the announcement of the award.
- Investigation - concerning investigations into disciplinary or criminal matters.
- Management - concerning policy and planning affecting the interests of groups of staff.
- Medical - medical reports and records and material relating to them.
- Personal - material only to be seen by the person to whom it is addressed.
- Policy - concerning proposals for new or changed Government policy before publication.
- Private - information collected through electronic Government services to the public and relating to the individual or an organisation.
- Staff - containing Procedures for Transmitting Protectively Marked Documents
- Visits - concerning details of visits by, for example, royalty, Ministers or very senior staff.

Annex D: OSCR Retention Schedules

Type of record (description)	Known Best Practice	Disposal*	Legislation that applies
Proactive Communications			
1.1.1 Media Digest (press reports digest)	National Archives Records Management Retention Scheduling 8. Press and Public Relations Records (item 5)	7 years	n/a
1.1.2 Media Cuttings (press cuttings)	National Archives Records Management Retention Scheduling 8. Press and Public Relations Records (item 2)	1 month	NLA Terms and Conditions also apply
1.1.3 Image Library Records (board/ staff photography)	National Archives Records Management Retention Scheduling 8. Press and Public Relations Records (item 10)	1 year	
1.1.4 Internal Communications (Riverside Review / Comms chatter)	National Archives Records Management Retention Scheduling 8. Press and Public Relations Records (item 15)	3 years	
1.1.5 Events Organisation	National Archives Records Management Retention Scheduling 8. Press and Public Relations Records (item 11)	7 years	
1.1.6 Publications (proofing)	None. 1 year retention period discussed and agreed internally.	1 year	
1.1.7 Press Releases	National Archives Records Management Retention Scheduling 8. Press and Public	7 years	

	Relations Records (item 1)		
1.1.8 OSCR Website Development	None. 5 year retention period discussed and agreed internally.	5 years	
1.1.9 Publicity Campaigns	National Archives Records Management Retention Scheduling 8. Press and Public Relations Records (item 9)	7 years	
1.2 Official Enquiries and briefings			
1.2.1 Official Enquiries (FOI/ DP/ ROPSI)	National Archives Records Management Retention Scheduling 14. FOI Model retention schedule	3 years	
1.2.2 Parliamentary Questions (PQs)	n/a. A permanent record is kept by the Scottish Parliament, in the daily “Written Answers Report”	5 years	
1.2.3 Official Briefings (MSPs, Committees)	None. 5 year retention period discussed and agreed internally.	5 years	
1.2.4 Media Briefing (Press Statements)	National Archives Records Management Retention Scheduling 8. Press and Public Relations Records (item 6)	7 years	
1.2.5 External Enquiries (Sales/ Marketing)	None. 1 year retention period discussed and agreed internally.	1 year	
1.3 ICT issues	None. 5 year retention period discussed and agreed internally.	5 years	
2.0 Policy Development			
2.1 Procedures	None. 5 year retention period discussed and agreed internally. Procedures Manual documents	5 years	

	and supporting documentation are marked for permanent preservation.		
2.2 Publications Library	None. Permanent preservation discussed and agreed	Permanent	
2.3 External agencies (liaison)	Scottish Government records Management Manual (2005) (3 Correspondence)	5 years	
2.4 Corporate Policies	None. 7 year retention period discussed and agreed internally	7 years	
2.5 Charity Law Policy Development	Scottish Government Records Management Manual (2005) (1 Policy: Policy on main records of branch)	1st Review in 12 years	
2.6 Contributing to legislation or standards	Scottish Government Records Management Manual (2005) (2 legislation: Primary legislation in which branch has interest)	5 years	
2.7 Legal Library	Scottish Government Records Management Manual (2005) (2 legislation: Legislation where branch has lead role)	Permanent	
2.8 Research and Evidence	Scottish Government Records Management Manual (2005) (11 research: When branch commissioning research)	Permanent	
3.0 Senior Management			
3.1 Audit & Assurance			
3.1.1 Audit Committee meetings	National Archives Records	3 years	

	Management Retention Scheduling 11. Internal Audit Records (item 7)		
3.1.2 Internal audit	National Archives Records Management Retention Scheduling 11. Internal Audit Records (item 1)	6 years	
3.1.3 External audit	National Archives Records Management Retention Scheduling 11. Internal Audit Records (item 7)	6 years	
3.1.4 Accountable Officer	None. Retention period agreed by CEO.	Permanent	
3.2 Customer Feedback			
3.2.1 Compliments 3.2.2 Complaints 3.2.3 Unacceptable actions	National Archives Records Management Retention Scheduling 7. Internal Audit Records (item 5)	3 years	
3.3 OSCR Board			
3.3.1 Board Minutes and papers	None. Retention period agreed by SMT	Permanent	
3.4 Scottish Charity Appeals Panel	Scottish Government Records Management Manual (2005) (3 correspondence: specific case records)	10 years	
3.5 Business Strategy/ Development			
3.5.1 Strategic planning	None. None. 5 year retention period discussed and agreed internally.	Until strategy superseded	

3.5.2 Business planning 3.5.3 Financial Planning	None. 3 year retention period discussed and agreed internally.	3 years from end of planning cycle to which it relates.	
3.6 Corporate Knowledge management			
3.6.1 Records Management	National Archives Records Management Retention Scheduling 9: Information management Records (items 1, 2 and 12)	Permanent	
3.6.2 Team meetings	Scottish Government Records Management Manual (2005) (13 Office Procedures: Branch Meetings)	5 years	
3.6.3 Incoming Correspondence (Scanned)	None. 3 year retention period discussed and agreed internally.	1st review in three years	
3.7 OSCR Risk Register	None. Permanent retention period discussed and agreed internally.	Permanent	
3.8 SMT Minutes and papers	None. Permanent retention period discussed and agreed internally.	Permanent	
3.9 Management Reports	Scottish Government Records Management Manual (2005)	5 years	
3.10 Statistics and Data Collection	Scottish Government Records Management Manual (2005)	5 years	
4.0 Human Resources			
4.1 Speculative job applications	None. 1 month retention period discussed and agreed internally.	1 month	* Scottish Government is the primary record keeper
4.2 Training and development	None. 5 year retention period discussed and agreed internally.	5 years	* Scottish Government is the primary record keeper

4.3 Personnel files	None. 6 year retention period discussed and agreed internally.	6 years	* Scottish Government is the primary record keeper
4.4 Recruitment	None. 1 year retention period discussed and agreed internally.	1 year	* Scottish Government is the primary record keeper
4.5 HR Returns	National Archives Records Management Retention Scheduling 2: Employee Personnel records (Annual assessment reports – 5 years)	5 years	
5.0 Resource Management			
5.1 Estate Management	None. 5 year retention period discussed and agreed internally.	5 years	
5.2 Environmental Management	None. 5 year retention period discussed and agreed internally.	5 years	
5.3 Project Management	National Archives Records Management Retention Scheduling 6: Project Records (item 2)	10 years	
5.4 Current Year Accounts			
5.4.1 Accounting Systems	National Archives Records Management Retention Scheduling 3: Accounting Records	6 years	Scottish Public Finance Manual Annual accounts: Annex 2
5.4.2 Annual Accounts	National Archives Records Management Retention Scheduling 3: Accounting Records	6 years	Scottish Public Finance Manual Annual accounts: Annex 2
5.4.3 Expenditure	National Archives Records Management Retention	6 years	Scottish Public Finance Manual Annual accounts: Annex 2

	Scheduling 3: Accounting Records		
5.4.4 Fixed Assets	National Archives Records Management Retention Scheduling 3: Accounting Records	6 years	Scottish Public Finance Manual Annual accounts: Annex 2
5.4.5 Journals	National Archives Records Management Retention Scheduling 3: Accounting Records	2 years	Scottish Public Finance Manual Annual accounts: Annex 2
5.4.6 Management Accounts	2 year retention period discussed and agreed internally (this is beyond the 1 year recommended by NA)	2 years	
5.4.7 Payroll	National Archives Records Management Retention Scheduling 3: Accounting Records	2 years	Scottish Public Finance Manual Annual accounts: Annex 2
5.4.8 Suppliers	National Archives Records Management Retention Scheduling 3: Accounting Records	2 years	Scottish Public Finance Manual Annual accounts: Annex 2
5.4.9 Travel and Subsistence			
5.5 Finance History	See 5.4 above		
5.6 Next financial year	See 5.4 above		
5.7 Purchasing			
5.7.1 Collaborative contracts	National Archives Records Management Retention Scheduling 5: Contractual	6 years	

	Records (item 21)		
5.7.2 Contract Management	National Archives Records Management Retention Scheduling 5: Contractual Records (item 21)	6 years	
5.7.3 Procurement (High) 5.7.4 Procurement (Low)	National Archives Records Management Retention Scheduling 5: Contractual Records (item 10)	6 years	
5.7.5 Unsuccessful tenders	National Archives Records Management Retention Scheduling 5: Contractual Records (item 9)	1 year	
6.0 Monitoring, Investigation and Compliance			
6.1 Annual Monitoring Programme			
6.1.1 Monitoring exception testing casework	None. 5 year retention period discussed and agreed internally.	5 years	
6.1.2 Monitoring advice	None. 5 year retention period discussed and agreed internally.	5 years	
6.1.3 Section 19 Casework	None. 5 year retention period discussed and agreed internally.	5 years	
6.1.4 QP letters	None. 5 year retention period discussed and agreed internally.	5 years	
6.2 Investigations and Compliance			
6.2.1 Investigation and compliance casework	None. 5 year retention period discussed and agreed internally.	5 years	
6.2.2 Investigations and compliance advice	None. 5 year retention period discussed and agreed internally.	5 years	
6.2.3 Applications for waiver of	None. 5 year retention period	5 years	

disqualification	discussed and agreed internally.		
6.3 MIC Outreach			
6.3.1 MIC Operational projects	None. 5 year retention period discussed and agreed internally.	5 years	
6.3.2 Compliance Support with intermediaries	None. 5 year retention period discussed and agreed internally.	5 years	
6.3.3 MIC Themed Studies	None. 5 year retention period discussed and agreed internally.	5 years	
7.0 Registration and Status			
7.1 Status – Applications			
7.1.1 Status Applications	None. 5 year retention period discussed and agreed internally.	5 years	
7.1.2 Status Advice	None. 5 year retention period discussed and agreed internally.	5 years	
7.2 Status – Rolling Review			
7.2.1 Rolling Review of Charitable Status case Files	None. 5 year retention period discussed and agreed internally.	5 years	
7.2.2 Rolling Review Pilot case Files (2007)	None. Permanent retention period discussed and agreed internally.	Permanent	
7.3 Consents and Notifications			
7.3.1 Consents and Notifications Case Files	None. 5 year retention period discussed and agreed internally.	5 years	
7.3.2 Consents and Notifications advice	None. 5 year retention period discussed and agreed internally.	5 years	
7.4 Scottish Charity Title Files	None. 5 year retention period discussed and agreed internally.	1st Review after 5 years	
7.5 Designated Religious Charities (DRC) Applications	None. 5 year retention period discussed and agreed internally.	5 years	

7.6 Designated National Collectors (DNCs)	None. 5 year retention period discussed and agreed internally.	5 years	
7.7 Registration and Status Operational Projects	None. 5 year retention period discussed and agreed internally.	5 years	
8.0 Annual submission and keeping the register			
8.1 Annual return and accounts queries	None. 5 year retention period discussed and agreed internally.	5 years	
8.2 Enquiries about charitable status	None. 2 month retention period discussed and agreed internally.	5 years	
8.3 'Orphan' accounts 8.4 'Orphan' accounts	None. 3 year retention period discussed and agreed internally.	3 years	
8.5 Annual Return non-submission casework	None. 5 year retention period discussed and agreed internally.	5 years	
8.6 Annual return and Monitoring return submissions by charities	None. 7 year retention period discussed and agreed internally.	7 years	
8.7 Scottish Charity Data			
8.8 Daily Register upload	None. 6 month retention period discussed and agreed internally.	6 months	

* Disposal is typically from date file closed.

Exceptions
Documents within categories 2.3, 2.6, 3.6.3 and 8.6 are disposed of based on the creation date of the document.