

REGISTERS OF SCOTLAND
Executive Agency



Information about Scotland's land & property

**REGISTERS OF SCOTLAND
DOCUMENT
AND
RECORDS MANAGEMENT
POLICY**

Contents

1. INTRODUCTION AND DEFINITIONS.....	3
2. SCOPE OF THE POLICY.....	4
3. REQUIREMENTS.....	5
4. LEGISLATION AND REGULATIONS.....	7
5. PRESERVATION.....	8
6. FILING AND CLASSIFICATION.....	11
7. ACCESS.....	12
8. SECURITY.....	13
9. POLICY REVIEW.....	14

1. Introduction and Definitions

1.1 Introduction

- 1.1.1 The purpose of this document is to set out a policy framework for the management of documents and records within the Registers of Scotland (the Agency). The policy applies to all media currently used within the Agency and which may be used in the future held across all its systems.
- 1.1.2 The policy is founded upon the principle that all information held across the Agency's systems is the property of the Agency and is managed by its staff for the benefit of the Agency.
- 1.1.3 The policy brings together prior Agency practices and incorporates government guidelines and acknowledged best practice in this field. The policy is viewed as a living document subject to review and additions and will adapt to changes in requirement and practice in the course of time.
- 1.1.4 The policy is supported by a further document – the Document and Records Management Practices and Procedures Guidelines – which addresses the aspects of this policy in the required level of detail.
- 1.1.5 The inclusion of documents as well as records in the policy is an acknowledgement of the nature of the Agency's business where documents may be in circulation for a considerable time before they attain the status of a record if they indeed ever do. There are, therefore, issues of document integrity and security which should be contained within the policy.
- 1.1.6 The policy is a general policy and is not restricted to electronic records alone. Although the management system for documents and records will be an electronic system the documents and records themselves may be in any media. Specific mention will be made to electronic records only when necessary.

1.2 Definitions

- 1.2.1 The following definitions are taken from BS ISO 15489-1 and pertain to the policy document, a full glossary of document and records management terms for use within the Agency will be developed over time and incorporated in the Document and Records Management Practices and Procedures Guidelines:

Document – recorded information or object which can be treated as a unit¹

Metadata – data describing context, content and structure of records and their management through time

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 business²

Records Management – field of management responsible for the efficient and systematic control of the creation, receipt, maintenance,

¹ These may include paper documents, digital scanned images of paper documents, electronic documents and e-mail,

² Records are documents whose authenticity and reliability must be preserved for a specified period of time.

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

Records System – information system which captures, manages and provides access to records through time

In addition, the following terms are used which have specific meaning within this document:

Corporate Assets – are those assets, physical, financial and intellectual, deemed to belong to the Agency as a corporate entity.

Corporate Records – definitive records of activities, actions or decisions pertaining to the operational functions or the governance of the Agency held as part of the Corporate Assets.

Personal Records – are any business related records which are held by staff for their own or localised purposes³. No documents of a personal nature which are not business related should be held on any Agency systems including the users' Home Folders.

Maintained – records are said to be maintained when systems are in place to ensure their continuing integrity as corporate assets.

2. Scope of the Policy

2.1 This Policy aims to meet the requirements for good management of all documents and records received by and created by the Agency, irrespective of media, both present and future. The policy covers:

- the requirements that must be met for the secure handling and management of all documents received by the Agency
- the requirements that must be met for the secure handling and management of all documents created within the Agency
- the requirements that must be met for the records themselves to be considered as a proper record of the activity of the organisation
- the requirements for systems and processes that deal with documents and records, the quality and reliability of which must be maintained to provide a valuable information and knowledge resource for the whole organisation
- the resources needed to preserve the record intact
- the filing and classification process for documents and records
- access to documents and records
- security of documents and records
- guidelines for reviewing the policy and checking the quality of implementation.

2.2 This policy governs all documents and records held by the Agency and its staff, irrespective of their media or mode of storage. This includes documents and records held on the Agency's network system and all its applications.

³ For example: PDS forms, performance statistics etc.

3. Requirements

3.1 Documents and records within the Agency must be preserved and stored for the required period. They will be selected using defined selection criteria and can be transferred to other organisations for future preservation, or destroyed once they are no longer of operational use. In order to ensure that the information constitutes a record the Agency is required at all times to ensure that:

- the document or record exists⁴
The information needed to reconstruct activities and transactions that have taken place is recorded.
- the document or record can be accessed
It is possible to locate and access the information and present it in a way that is true to the original presentation of the information
- the document or record can be interpreted⁵
A context for the information can be established showing when, where and who created it, how it was used and how it is related to other information
- the document or record can be trusted
The information and its representation exactly matches that which was actually created and used, and its integrity and authenticity can be demonstrated beyond reasonable doubt
- the document or record can be maintained
The record can be deemed to exist and can be accessed, interpreted and trusted for as long as necessary and remain so on transfer to other approved locations, systems and technologies.

3.2 The Agency deems that documents and records are an asset that require careful control and the diligent application of the following standards to all systems and processes within the organisation. The systems and processes will be required to:

- identify whether they deal with documents, electronic documents, records, electronic records or potential electronic records
- if they do deal with such documents or records, the system or process must maintain them so that the record nature remains intact
- provide information on the documents, records or potential records as required for inclusion as part of a collection in the inventory of record collections, part of the Inventory of Information Assets.
- provide the document and records for filing and classification, transfer or disposal according to the records management guidance
- keep the records secure and monitor access in accordance with the Agency Security Policy, BS7799/ISO17799 and records management guidance
- have regard for legal requirements such as Data Protection, Freedom of Information and copyright legislation.

⁴ An Inventory of Information Assets is required for compliance with BS7799/ISO17799 and is a prerequisite for an effective records management system

⁵ The Agency will comply with the e-Government Metadata Standard Version 2 published by the Cabinet Office, Office of the e-Envoy.

3.3 In particular, during the process of any move to a fully integrated electronic system of document and records management, the Agency will monitor electronic records and potential electronic records to ensure that:

- records that should be captured are being processed electronically if they do not appear in the paper record
- there is no unwarranted duplication between the paper and electronic record collections
- there is a distinction made between the electronic documents which are printed, printed records that reside in the paper record systems and other original documents that are retained as electronic records (possibly to be passed to an electronic record keeping system)
- an inventory of all Agency record collections, part of the Inventory of Information Assets, will be created to ascertain the nature and type of records and potential records within collections. Care must be taken to ensure a good level of control of the record creating systems and that the records nature is preserved appropriately in the transitional period
- the implementation of any Record Management System should clearly show where the record is located and in which form it is held.

4. Legislation and Regulations

- 4.1 The policy complies with the following Acts, regulations and best practice standards:
- Data Protection Act 1998
 - Freedom of Information (Scotland) Act 2002
 - Electronic Communications Act 2000
 - Code of Practice on Records Management to the Freedom of Information (Scotland) Act 2002
 - Model Action Plan for developing records management arrangements compliant with the Code of Practice on Records Management
 - Copyright Designs and Patents Act 1988
 - BS/ISO15489 on Records Management
 - BS7799/ISO17799 on Information Security
 - PD0008 – Code of practice for legal admissibility and evidential weight of information stored electronically (BSI)
 - PD0010 – Principles of Good Practice for Information Management (BSI)
 - PD0025:1 & 2 – Guidelines for BS/ISO 15489
 - e-Government Metadata Standard Version 2
 - Government Category List
- 4.2 In addition, certain documents and records will be subject to legislation covering their specialist subject area.

5. Preservation

5.1 The following principles for preservation of, and long-term access to, the Agency's corporate records, do not attempt to describe strategies. Their purpose is to provide a basis upon which strategies for preservation of, and long-term access to, Agency records will be founded. Neither is there any attempt to indicate how decisions regarding 'significance' will be determined.

5.1.1 Co-operation

The co-operation of all staff with a role in the generation, use, management, distribution and preservation of records is essential.

Continuing access to records will be dependent on the co-operation of record creators, record management, system designers/suppliers, Intranet/Internet publishers, record users and the management groups and boards.

5.1.2 Role of Creator

Creators of records have the initial, and in some cases, a continuing role in preserving access to them.

Unless creators take initial steps to facilitate ongoing access to their material, access may be lost or the ability of a Record Management function to take responsibility for preserving access may be severely inhibited. Therefore, it is the absolute responsibility of the creator to save a document or record to the appropriate part of the Agency File Plan and to ensure it is accessible by all authorised staff. It is not permitted to save final versions of Corporate Documents and/or Records to the creators Home Folder. Declaring a document to be a record is a formal point of transition at which it passes into corporate ownership.⁶ (Once designated as a record the document is no longer managed by the creator but by a Record Management function, on behalf of the Agency as part of its corporate information resource – see 5.1.7).

5.1.3 Distributed Responsibility

Creators/users of records need to be aware of their roles and responsibilities.

Positive action, and the application of stringent information management disciplines, is required to capture, document and maintain information as records which demonstrate reliability and authenticity. Thus, the policy, associated practices and guidelines, will be described in appropriate detail, widely disseminated, and inform procedures and practices.

Within the electronic environment, in addition to the advantages offered by greater flexibility and access to information, the balance of responsibility, for capturing, filing and effectively using electronic records, shifts towards the

⁶ The information contained in the records constitutes a corporate rather than an individual resource, and as such the declaration process acknowledges and confirms this principle.

creator/user. In such an environment, the record manager becomes less concerned with acting as an intermediary between the creator/user and the record, and more with influencing the environment in which record handling occurs.

The quality of the record, therefore, is the responsibility of the creator. The records manager is responsible for the continuing integrity and preservation of that record alone. Any changes to the contents of an existing record result in the commencement of a fresh record creating process which will result in the creation of a new record, subject to all due process.

5.1.4 Appraisal – retention, disposal, and archive

Access to records should be preserved only for as long as they are judged to have continuing value and significance. Records show whether the Agency, or responsible individuals within it, have met defined legal and organisational obligations.

The retention and disposal schedules for all Agency records will be established to meet the relevant legal and corporate requirements. A full schedule will be developed and included in the Document and Records Management Practices and Procedures Guidelines. The Draft Code of Practice on Records Management to the Freedom of Information (Scotland) Act 2002 requires that records disposal (defined as the point in their lifecycle when they are transferred to the NAS or destroyed) is undertaken in accordance with clearly established policies which have been formally adopted throughout the Agency, and which are enforced by properly authorised staff.

5.1.5 Rights

The rights of creators, users, and subjects of records, need to be carefully balanced and protected in accordance with the principles of the Freedom of Information (Scotland) Act 2002, the Data Protection Act 1998 and the Copyright Designs and Patents Act 1988

5.1.6 Strategies

With regard to completeness, a strategy will be required to consider how to manage a relationship between electronic⁷ and paper records.

Electronic records will need to be migrated through successive upgrades of hardware and software. Strategies to preserve access to electronic records must consider how to protect the integrity and functionality of these records. Strategies to preserve access to electronic records will also need to be periodically reviewed and modified to reflect best practice current at the time.

5.1.7 Responsibility for Records Management

In accordance with the Draft Code of Practice on Records Management to the Freedom of Information (Scotland) Act 2002, records management is recognised as a specific corporate function within the Agency.

⁷ The fragile nature of the electronic medium, and the dynamic way in which information technology is deployed, threaten the reliability and authenticity of the record if appropriate record management disciplines are not applied.

This function brings together the responsibilities for all records held by the Agency, throughout their life cycle, from planning and creation through to ultimate disposal. The person responsible for the records management function (the Records Manager) will also be responsible for, or have a close working relationship with, the person(s) responsible for Data Protection, Copyright Issues and FOI.

5.1.8 Role of the Management Board

Records are an essential element of good governance. They provide a sound basis to assure the accountability of the Agency over time.

By extending knowledge of past actions and decisions to inform future decision-making they provide a valuable repository of information for future boards. It is therefore the role of the Board to promote the appropriate policy regimes to ensure it fulfils its regulatory and legislative responsibilities. It is also the role of the Board to develop and support the appropriate regime for continuing and equitable access to its records.

5.2 The Agency will preserve all records during any change in the infrastructure so that they can still satisfy the original policy requirements. Preservation needs must be satisfied when there are changes in:

- the technology that processes the electronic records, how this affects the way records are processed throughout the records' existence
- organisational structures and how these are interpreted and give the records context
- the definition of terms used in the metadata and within the records themselves
- the classification of the electronic records including how the records are grouped and described so that they can be presented in a way consistent with the original understanding of the subject when the record was created.

6. Filing and Classification

- 6.1 The approach the Agency has to Filing and Classification is governed by the e-Government Metadata Standard Version 2⁸, and involves:
- classifying documents and records by appropriate levels of confidentiality, integrity and availability
 - classifying of documents and records into series that have meaningful titles and a consistent reference code
 - setting a responsibility on individuals forming record items to allocate them to a series and if necessary a sub-series or sub-sub-series
 - having sequences of reference numbers that can cover series with both electronic and paper records
 - checking that the correct records have been allocated to the sequence and that meaningful titles are used
 - auditing lists of the references used so that the filing and classification system makes sense and records can be found in appropriate search sequences.

⁸ This has now been updated to Version 3.1 and the Agency will review the its application as part of an EDRMS post implementation review.

7. Access

7.1 The Agency will use access controls to allow documents and records to be viewed by the appropriate parties.

7.2 Access control factors include:

- all records are part of the corporate knowledge. Unless restricted, they will be made readily available within the organisation. This may be subject to volume restrictions because of technical limitations or copyright reasons
- electronic records will be made available for continuity of actions. The creators and managing individuals or groups should have access to relevant information
- roles or bodies within the Agency which have been identified as being able to make an accurate judgement will decide on the levels of access to the record. This judgement may be on a whole series or simply cover individual items. It will identify any restrictions on the records and it will highlight any groups or individuals within the organisation who should have access
- any judgements, including any background reasons for withholding or masking information within the record or record series, are to be recorded. The resulting record will be kept for at least as long as the records in question; however it may not have the same access status as the main record
- in considering whether records can be disclosed or withheld, the Agency will not be unduly restrictive and will comply with the Freedom of Information (Scotland) Act 2002 and the Data Protection Act 1998.
- information taken from the records or record metadata may be subject to legislation requiring it to be either withheld or made more widely available outside normal business needs (or even outside the organisation itself). For example there is a need to comply with Data Protection and Freedom of Information legislation.
- any access arrangements will be made for a specified duration and these will be reviewed according to a schedule identified during appraisal.

8. Security

8.1 The Agency will take all reasonable steps to ensure that documents and records and processes dealing with them are secure. Once recorded and entered in the system, they will be safe from alteration or loss and interpretation will be assisted by the provision of context.

8.2 The steps include:

- enabling staff to comply with records management best practice
- using a corporate policy and organisational procedures, where they exist, and helping to determine new policy and procedures where they do not
- training staff to use the records management systems for an accurate representation of the records using only relevant metadata, thereby ensuring consistency in record registration and metadata without loss of context and control
- auditing the systems to trace any deviation from procedure
- offering solutions to rectify mistakes or altering the procedures to accommodate better ways of working
- enforcing access restrictions with user IDs and passwords, setting user lockouts
- maintaining business continuity plans, in accordance with the Agency Risk Management and Business Continuity Policies, that include replicating electronic records on a physically secure back-up and safeguarding the information from technical failures.
- implementing strict back-up cycles with updates for new records and metadata, ensuring that any destroyed or transferred records are also promptly physically cleaned from the back-ups
- labelling the replicated records as a replica set and making sure these cannot be used as the master set, unless the original has been destroyed accidentally or following a disaster

9. Policy Review

- 9.1 The Agency will follow the policy within all relevant procedures and guidance used for operational activities. Interpretation of the policy will be monitored and there will be a regular planned audit to review how the policy is being put into practice.
- 9.2 The audit will seek to:
- identify areas of operation that are covered or not covered by the policy and to identify which procedures and/or guidance should adhere to the policy
 - follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of electronic records and use a subsidiary development plan if there are major changes to be made
 - set requirements by implementing new procedures, including obtaining feedback where the procedures do not match the desired activity
 - highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures such as security and access.