Risk Management Authority

Records Management Plan

RMA

Risk Management Authority

Working towards a Safer Scotland

Contents Page

1. Introduction

1.1 Background

The Public Records (Scotland) Act 2011 (hereafter referred to as ‘the Act’) came into force in January 2013. The Act obliges the Risk Management Authority (RMA) as a public authority to prepare and implement a Records Management Plan (RMP). This RMP sets out the proper arrangements for the management of the RMA’s public records to the Keeper of the Records of Scotland (“the Keeper”) for his agreement under section 1 of the Act.

It is important to note that operating effective records management arrangements delivers significant benefits for the RMA - for example it helps to:

- increase efficiency and effectiveness, delivering savings in administration costs;
- improve and develop service delivery;
- achieve business objectives and targets;
- ensure compliance with the Public Records (Scotland) Act 2011 and other legislative requirements, standards and codes of conduct; and
- support transparency and open government.

The RMA’s Records Management Plan is based upon the Keeper’s published Model Records Plan and covers 14 Elements, which are:

1. Senior management responsibility
2. Records manager responsibility
3. Records management policy statement
4. Business classification
5. Retention schedules
6. Destruction arrangements
7. Archiving and transfer arrangements
8. Information security
9. Data protection
10. Business continuity and vital records
11. Audit trail
12. Competency framework for records management staff
13. Assessment and review
14. Shared information

More information about the Public Records (Scotland) Act 2011 can be found on the National Records of Scotland website: http://www.nas.gov.uk/recordKeeping/publicRecordsActIntroduction.asp

A copy of the Act can be viewed online via the National Archives website:
http://www.legislation.gov.uk/asp/2011/12/part/1/enacted

1.2 Records Management in the RMA

The records of the RMA constitute an auditable account of the authority’s activities, which provides evidence of the business, actions, decisions and resulting policies produced by the RMA.

Records represent a vital asset, which support the daily functions of the RMA and protect the interests and rights of staff, stakeholders and members of the public who have dealings with the RMA. Effective record keeping supports efficiency, consistency and continuity of work and enables the RMA to deliver sustainable services. It ensures that the correct information is created, stored, maintained, retrieved and destroyed or preserved in accordance with business need and statutory and legislative requirements.

Effective records management assists the RMA to achieve its outcomes and contribute to our strategies as set out in our Corporate Plan. Records Management in the RMA is underpinned by our Records Management Policy and Procedure, which are based upon the requirements of the Public Records (Scotland) Act 2011 and records management best practice.

1.3 Records covered by this plan

In line with the Act, **all** records created in the carrying out of the RMA’s functions (whether directly or by third parties) are public records. Part 1, section 3.1 of the Act states that:

“… “public records”, in relation to an authority, means—
(a) records created by or on behalf of the authority in carrying out its functions,
(b) records created by or on behalf of a contractor in carrying out the authority’s functions,
(c) records created by any other person that have come into the possession of the authority or a contractor in carrying out the authority’s functions.”

1.4 Records Management systems in the RMA

The RMA uses three main types of records management systems:

- Manual Filing System (where it is necessary to keep paper and other physical records)
- G Drive for IT applications and databases (that process records for specific functions)
- Electronic Record and Document Management System (eRDM)

All records management systems are subject to the records management procedure.

2.0 Elements of the Plan

2.1 Element 1: Senior Management Responsibility

Identify an Individual at Senior Level Who Has Overall Strategic Responsibility for Records Management

Senior Management responsibility for Records Management within the RMA lies with:

Paul Keoghan
Director of Business Performance
The Risk Management Authority
7 Thread Street
Paisley
Renfrewshire PA1 1JR
Tel: 0141 278 4478
Email: info@rmascotland.gsi.gov.uk

2.2 Element 2: Records Management Responsibility

Identify Individual Within the Authority, Answerable to Senior Management, to have Day-to-Day Operational Responsibility for Records Management Within the Authority

The point of contact for the operation of records management within the RMA is:

Paul Foy
Governance & Communications Administrator
The Risk Management Authority
7 Thread Street
Paisley
Renfrewshire PA1 1JR
Tel: 0141 278 4478
Email: info@rmascotland.gsi.gov.uk

Evidence:
Letter from the Chief Executive covering elements 1, 2 and 3

2.3 Element 3: Records Management Policy Statement

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 RMA's commitment to effective records management is set out in its Records Management Policy and Procedure. The objective of these documents is to ensure that appropriate systems and good governance arrangements are in place for the management of the RMA's records and information. Records are defined as 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.

Background

The RMA was established in 2005 under the Criminal Justice (Scotland) Act 2003, for the purpose of ensuring the effective assessment and minimisation of risk. Our functions include the communication of best practice, drawing evidence from national and international research and development programmes to improve risk assessment and risk management approaches in Scotland. The RMA is sponsored by the Parole Unit of the Justice Directorate and operates to an agreed structure known as a Sponsorship Framework. This Framework sets out the RMA's overall aims, objectives and targets in support of the Scottish Ministers' wider strategic aims; and the rules and guidelines relevant to the exercise of the RMA's functions.

The Public Records (Scotland) Act 2011 (hereafter referred to as 'the Act') came fully into force in January 2013. The Act obliges the RMA to prepare and implement a records management plan (RMP). The RMP sets out proper arrangements for the management of records within the RMA and is agreed with the Keeper of the Records of Scotland (the Keeper).

The Freedom of Information (Scotland) Act 2002 provides a general legal right of access for anyone to the information held by all public authorities, subject to certain exclusions. The Data Protection Act (1998) provides access to data subjects to their personal information held by organisations. Therefore, we need to ensure that our records are appropriately ordered, readily accessible and able to be shared with the public when relevant.

Overview of RMA records management processes

Records management is about controlling records within a comprehensive regime made up of policies, procedures, systems, processes and behaviours. Together they ensure that reliable evidence of actions and decisions is kept and remains available for reference and use when needed, and that the RMA benefits from effective management of one of its key assets, its records.

The RMA's aim to ensure good records management practice that:

- Helps staff to do their job better: it supports ease and efficiency of working because staff can find the information they need, when they need it;
- Protects the RMA and its staff: it provides evidence of people's rights and entitlements, and shows what the RMA did and why it did it;
- Saves time by ensuring information can be found easily;
- Reduces costs by ensuring the RMA doesn't keep any more records than it has to, and staff know when they can delete or destroy them;
- Provides records that can be relied on, both by helping staff to find the appropriate version and, by giving records a high value as evidence if they are needed in a court of law.

The RMA uses three main types of records management systems:

- Manual Filing System (where it is necessary to keep paper and other physical records)
- G Drive for IT applications and databases (that process records for specific functions)
- Electronic Record and Document Management System (eRDM)

All records management systems are subject to the records management procedure.

eRDM is the electronic Record and Document Management system, managed and supported by the Scottish Government, which is used by the RMA to manage its official records and related documents. eRDM impacts upon the way that each member of staff works across the RMA and it helps staff to share information and records in a more structured, efficient and effective way. eRDM enables staff to create, store, amend, archive and retrieve information electronically, providing an office-wide information and knowledge sharing resource which is designed to facilitate efficiencies in the creation, sharing, retention and retrieval of information. It also assists the RMA to comply with compulsory legislative requirements.

Next steps

The RMA relocated to new office premises in December 2013. This relocation prompted a review of existing records management processes and identified the requirement for the RMA to move to an eRDM system. The implementation of this system will continue throughout 2014 and is included as an objective in the RMA's Business Plan 2014-15. The RMA's Records Management Policy and Procedure have been revised to support the implementation of this new system. Implementation will involve the further development of a file plan and business classification system, and the delivery of staff training to ensure that the RMA's records management is operated effectively and efficiently.

The RMA's revised Records Management Policy and Procedure and Records Management Plan will be officially approved by the Senior Management Team and Board, and will thereafter be reviewed annually.

Evidence:
RMA Records Management Policy
RMA Records Management Procedure

2.4 Element 4: Business Classification

A business classification scheme describes what business activities the authority undertakes – whether alone or in partnership.

As part of the move to eRDM, the RMA is currently developing a business classification scheme and file plan covering all functions of the RMA. The RMA has adapted the Local Government Classification Scheme as the basis for its business classification scheme and file plan.

The eRDM system is structured by a file plan that supports the business activities of the RMA. This file plan underpins the RMA's business classification scheme; identifying the folders (files) and records in a structure that is based upon the functions and activities of the RMA. This functional approach focuses on managing records according to their business context and is a hierarchy of terms, moving from the broadest level function to the more specific activity.

In simple terms, entries are classified according to:
Function, then
Activity, then
Transaction.

The RMA's file plan identifies three main functions, which reflect the business activities of the RMA. These being:

Offenders
Research and Development
Corporate

The implementation of eRDM within the RMA requires that the file plan is developed in line with existing Scottish Government structures to accommodate strict security models, whilst facilitating information sharing, and the application of retention scheduling.

Evidence:
Draft file plan

2.5 Element 5: Retention Schedules

A retention schedule is a list of records for which pre-determined destruction dates have been established.

All RMA information should be stored in repositories which have an official retention and disposal schedule attached to them. Each file, whether virtual or physical, has an allocated file type (policy, casework etc) which determines when a file should be closed and destroyed. The RMA eRDM system provides the framework for the retention and disposal arrangements of electronic files, outlining the procedure for each type of record as per the eRDM 'file type' guidance document.

The RMA's eRDM system is managed by the Scottish Government. This system has inherent retention and disposal arrangements, underpinned by File Type Guidance – all records when created are set with a specified file type; once set, this file type cannot be amended. The file type identifies the information contained and details the set restrictions, retention schedule and disposal arrangements for each record.

These retention schedules will be mirrored by the RMA for records held in manual filing systems (where it is necessary to keep paper and other physical records) and G Drive for IT applications and databases (that process records for specific functions that cannot be stored on eRDM).

Evidence:
eRDM Operations File Type Guidance

2.6 Element 6: Destruction Arrangements

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.

The RMA has a contract with Shred-it Ltd. to provide a secure mobile shredding service for the destruction of confidential material.

This service provides:

- Secure, locked consoles in RMA offices
- Regularly scheduled collection by uniformed, security-screened staff (4 weekly)
- On site cross-cut shredding in Shred-it locked trucks
- Multiple shred sizes
- Secure chain-of-custody
- Certificate of Destruction
- Recycling by approved partners to reduce carbon footprint

Shred-it uses cross cut shredding technology so that information cannot be reproduced or recreated, ensuring that confidential information will stay secure. This process of cross cut shredding offers greater security than conventional strip-cut shredders, which can leave important information visible even after shredding. In contrast, documents are shredded into confetti-sized pieces that cannot be reconstructed, ensuring total destruction of confidential documents. Documents are never sorted before shredding, there's a secure chain-of-custody from collection to the time they are destroyed, and a Certificate of Destruction is produced when the shredding is complete as proof of RMA compliance with data protection best practices.

Evidence:
Shred-It Ltd waste transfer document

2.7 Element 7: Archiving and Transfer Arrangements

This is a 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.

The RMA was established in 2005 under the Criminal Justice (Scotland) Act 2003. As a relatively young organisation, the RMA has yet to transfer any records to an appropriate archiving repository. As part of the move to eRDM, the RMA will identify records of enduring value and develop archiving mechanisms and arrangements, informed by the retention schedules inherent to the eRDM file type guidance.

As part of the relocation to new office premises in December 2013, all manual paper RMA records were forwarded to the Scottish Government Central Scanning Unit to convert them into electronic files. These files will be transferred into the RMA’s eRDM system.

2.8 Element 8: Information Security

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 records.

The RMA takes the security of information very seriously and seeks to protect its information assets from all threats, whether internal or external, deliberate or accidental. The RMA protects information through the operation of a Security Policy and Procedure. The primary purpose of the guidelines contained in these documents is to provide clear policy direction and management support on the implementation and maintenance of information security.

Key elements of the Security Procedure include staff guidance on security breaches, IT security, clear desk policy, Government Classification system (protective markings) and building / entry procedures. Advice and support on all security procedures is provided to staff by the RMA's SIRO (Senior Information Risk Owner).

As a minimum requirement all staff are subject to recruitment controls known as the Baseline Personnel Security Standard (BPSS). The purpose of personnel security procedures is to provide a level of assurance as to the trustworthiness, integrity and reliability of all RMA employees, contractors and temporary staff.

A Protecting Information Level 1 eLearning course is mandatory for all staff to complete. This training provides staff with a comprehensive guide to why information is so important, the risks to its safety, and what can be done to protect it.

The RMA's ICT systems are provided by the Scottish Government's Information Services and Information Systems Division (ISIS). The range of services provided by ISIS to the RMA include SCOTS desktop IT services infrastructure such as computer hardware, access to the Government Secure Intranet and the Internet. RMA staff are therefore required to adhere to the Scottish Government IT Code of Conduct, which provides guidance on the use of SCOTS, email and the internet

Evidence:
RMA Security Policy
RMA Security Procedure
Scottish Government IT Code of Conduct
Protecting Information Level 1

2.9 Element 9: Data Protection

An authority that handles personal information about individuals has a number of legal obligations to protect that information under the Data Protection Act 1998.

In order to deliver our statutory functions (which concern the effective assessment and minimisation of risk), the RMA requires to gather and process personal data. The Data Protection Act 1998 regulates the processing of personal data by the RMA. The Data Protection Act gives individuals the right to be advised of and receive copies of any personal data relating to them which is held by the RMA. The Data Protection Act is enforced by the UK Information Commissioner, who provides guidance and advice on complying with the terms of the Act and investigates complaints regarding possible breaches of the obligations contained within the Act. The Information Commissioner maintains a register of all Data Controllers in the UK, whereby Data Controllers are required to register the types of personal data processed by them, the purposes of that processing and the third parties with whom the personal data may be shared.

The RMA's registration can be viewed on the Information Commissioner's website, http://www.ico.gov.uk/ Registration number **Z9391486**.

The Data Protection Act 1998 sets out 8 data protection principles which must be complied with when the council is processing personal data. The 8 principles require that personal data:

- must be processed fairly and lawfully
- must be processed for specified and lawful purposes
- must be adequate, relevant and not excessive
- must be accurate and up to date
- must not be kept longer than necessary
- must be processed in accordance with the data subject's rights
- be held and processed securely
- must not be transferred to countries out with the EEA without suitable safeguards.

The Governance and Communications Administrator is the RMA's Data Protection Officer, responsible for responding to subject access requests under the Data Protection Act 1998 and freedom of information requests under the Freedom of Information (Scotland) Act 2002. The Governance and Communications Administrator is trained in data protection, data security, handling subject access requests and freedom of information to ensure that personal data is processed in accordance with the data protection principles.

Evidence:
ICO data protection register extract
RMA Data Protection Policy

2.10 Element 10: Business Continuity and Vital Records

A business continuity and vital records plan serves as the main resource for the preparation for, response to, and recovery from, an emergency that might affect any number of crucial functions in an authority.

The RMA operates a Business Continuity Plan. This plan may be invoked when an incident is considered likely to significantly affect the business operations of the RMA and relates to all business functions and services. It guides preparedness, response and recovery actions.

The RMA's vital records will be identified as part of the business classification scheme / eRDM file plan development and noted accordingly in subsequent reviews of the RMA's Business Continuity Plan.

Evidence:
RMA Business Continuity Plan

2.11 Element 11: Audit Trail

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.

Work will be undertaken to improve the procedures in place for creating audit trails that cover all transactions.

The eRDM (electronic records and document management) system when fully operational will provide electronic audit trails as evidence of viewing, modifying and deletion of records. The RMA's IT systems, provided and managed by the Scottish Government, provide audit logs that record usage and updates to email records. Paper records of an operational nature, such as Board and Committee papers and minutes are maintained on site and identified within restricted areas of the G drive. Movement of these paper records are controlled through a method of check-out/in – logs are kept of restricted documents issued to Board and staff members, which are then reconciled before being marked for destruction.

Electronic records currently held in the RMA's G drive are not held in a structured format, therefore these records do not have a managed audit trail. The G drive does not have a structured disposal schedule, therefore it has in principle an infinite 'shelf life' and as such does not comply with government information disposal policy. The G drive will therefore not be used for storing official records longer term. The G drive will eventually become 'read only', which means that whilst documents on the G drive can be accessed, saved to eRDM, or copy and pasted, no additional documents will be filed there.

However, the RMA does utilise a small number of databases to support the delivery of administrative functions, including a Contacts Database and Mail Log, therefore an area of the G drive will remain open for these records.

2.12 Element 12: Competency framework for Records Mgt Staff

A competency framework lists the core competencies and the key knowledge and skills by a records manager. It can be used as a basis for developing job descriptions, identifying training needs, and assessing performance.

The RMA Senior Information Risk Owner (SIRO) has direct responsibility for maintaining the Records Management Policy, providing advice and guidance on its implementation. The position of RMA SIRO is held by the Director of Business Performance. The point of contact for the day to day operation of records management is the Governance & Communications Administrator. As these members of staff have specific responsibilities for Information Management and Records Management, they have therefore undertaken training in Information Security Awareness, Data Protection and Freedom of Information.

It is the responsibility of each member of staff to adhere to the Records Management Policy. The RMA recognises that RMA assets are regularly accessed by Board members as part of their duties, therefore Board members are also expected to adhere to the procedures that support this policy. All staff must complete a mandatory Protecting Information training course, and an eRDM training course, to ensure that staff have an understanding and working knowledge of how records management systems are used in the RMA.

The RMA has a small structure of fourteen permanent employees and places great emphasis on the continued development of those staff members to support the achievement of our corporate and business plan objectives. The RMA seeks to encourage and support the potential of all staff members and invest in their continued professional development through the identification of training opportunities and attendance at relevant seminars and conferences. Staff are also subject to a comprehensive system of performance review and are encouraged to improve their skills and expertise on an ongoing basis as part of their work for the RMA.

Evidence:
Training information
eRDM training schedule
GCA Job description
DBP Job description

2.13 Element 13: Assessment and Review

Regular 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.

The Records Management Plan, Records Management Policy and Procedure are subject to the RMA's governance, monitoring and review process. As such, the plan will be assessed on an annual basis by the Governance and Communications Administrator and submitted to the Senior Management Team / RMA Board for review.

2.14 Element 14: Shared Information

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.

As part of our function to promote effective practice, the RMA periodically shares and receives information from relevant partners and stakeholders, primarily to support the delivery of national programmes or research. In these circumstances, a data sharing agreement is put in place. The RMA's data sharing agreements are based upon the ICO's Data Sharing Code of Practice.

Evidence:
Example data sharing agreement

Risk Management Authority
7 Thread Street
Paisley
PA1 1JR

tel. 0141 278 4478
email. info@rmascotland.gsi.gov.uk

www.rmascotland.gov.uk