Public Records (Scotland) Act 2011

The Mental Welfare Commission for Scotland
Records Management Plan

Introduction

The Commission's aim is to ensure that care, treatment and support are lawful and respect the rights and promote the welfare of individuals with mental illness, learning disability and related conditions. Our duties are set out in the Mental Health (Care and Treatment) (Scotland) Act 2003.

The Adults with Incapacity (Scotland) Act 2000 provides a framework for safeguarding the welfare and managing the finances of adults (people aged 16 or

over) who lack capacity due to mental illness, learning disability and related conditions.

We have supervisory, investigative and advisory duties under this Act in relation to welfare guardianship and welfare powers of attorney.

When the 2003 Mental Health Act came into effect in October 2005, the Commission developed an Integrated Information Management Portal (IIMP) in order to store information on the individuals it comes into contact with in the course of carrying out its duties under both the 2003 Act and the Adults with Incapacity (Scotland) Act. IIMP is also used to hold final versions of some of our corporate records. Information on individuals added to IIMP is checked before entry to ensure its accuracy. Retrieval of information from IIMP is fast and reliable (there has been less than 2 days' downtime since its introduction).

The Victims and Witnesses (Scotland) Act established a National Confidential Forum (NCF). The NCF will be established in July, 2014. The NCF will be a committee of the Mental Welfare Commission for Scotland but will operate independently and will be led by a Forum Head who will carry out hearings alongside up to three panel members.

The Forum will provide a means for persons who were placed in institutional care as children to describe in confidence experiences of that care and/or any abuse experienced during the period spent in that care.

As part of the enabling legislation, the NCF requires to have a Records Management Plan (RMP) which has been approved by the Keeper. Although the Commission's RMP has not been formally approved, the Commission aims to work with newly appointed NCF staff to establish an appropriate RMP which they will submit for approval to the Keeper.

Given that staff of the NCF will be Commission staff and therefore subject to the same policies and able to access expertise and guidance via the Commission, it is not anticipated that the NCF RMP will vary fundamentally from that of the Commission.

The Commission recognises its duties under the Public Records (Scotland) Act 2011 (PRSA) which was borne out of recommendations from the Shaw Report in 2007. The Act requires that the Commission, and other named authorities, prepare and implement a records management plan (RMP), which needs to provide evidence that it has proper and effective arrangements in place for the management of its records, for submission to the Keeper of the Records of Scotland.

The Commission is cognisant with the definition of a record contained in the PRSA, which includes records held in electronic and manual form, and on a range of media. While the Commission's records are mainly held electronically, including incoming correspondence and other paper documents which are scanned onto IIMP on receipt, paper copies of records are also produced. This document establishes the arrangements for the management of records within the Commission, in whatever form they take.

The Commission's Records Management Plan is based on the Keeper's published Model Records Plan. The model plan has 14 Elements and this RMP lists these and provides an explanation and or evidence of our compliance with each element, and our commitment to continuous improvement where we feel our current practice is not robust.

Our commitment

Implementation of the Records Management Plan will enable the Mental Welfare Commission for Scotland to ensure compliance with the Public Records (Scotland) Act 2011, Data Protection Act 1998 and Freedom of Information (Scotland) Act 2002.

The Commission recognises the importance of good records management practices to ensure:

- Sensitive records of people with mental illness, learning disability or related conditions are safeguarded
- Open Government
- Legal Compliance
- Accountability
- The rights of the Commission, its employees, stakeholders and the public are upheld
- Support for its decision making processes
- Business Continuity (including performance of statutory duties)
- Efficient and effective functions.

The guiding principle of records management at the Commission is to ensure that information is available when and where it is needed, in an organised and efficient manner, and in a well-maintained and secure environment.

The Commission's Records Management Plan will take effect from the date of sign off by the Keeper of the Records of Scotland and, because it is an iterative document, will be regularly reviewed and updated. It will be presented annually to our Board for formal review and approval.

The Elements

Element 1: Responsibility for the Records Management Plan

The Chief Executive, Mr Colin McKay, is the Data Controller for the Commission. He has delegated responsibility for the Records Management Plan to Alison McRae, Head of Corporate Services. Enquiries about the Records Management Plan should be routed through enquiries@mwcscot.org.uk or, alternatively, should be addressed to:

Mental Welfare Commission for Scotland
Thistle House
91 Haymarket terrace
Edinburgh

EH12 5HE
Tel: 0131 313 8777

Appendix 1 – Letter from the Chief Executive of the Commission

Element 2 : Records Manager responsibility

Alison Aiton, Information Manager, has operational responsibility for records management in the Commission. Her role includes the development and implementation of the Records Management Plan and, further, she will:

- Issue guidance and provide, or facilitate, training in records management to all staff
- Support users of records management systems
- Ensure the Commission's records management systems accord with best practice in the field
- Develop appropriate retention schedules and classification schemes
- Undertake compliance audits of records management programmes (policies, procedures and systems) to ensure the Commission meets its statutory obligations
- Develop strategies for the permanent preservation of selected records in conjunction with the National Records Scotland (NRS)

Enquiries relating to the operational aspects of records management should be routed through enquiries@mwcscot.org.uk or, alternatively, should be addressed to:
Mental Welfare Commission for Scotland
Thistle House
91 Haymarket terrace
Edinburgh
EH12 5HE
Tel: 0131 313 8777

Element 3: Records Management Policy

The Commission's has a Records Management Policy which is reviewed and presented to the Board annually for approval. Our current policy was approved in January, 2014. **Appendix 2 – Records Management Policy**

The purpose of our Records Management policy is to demonstrate the importance which the Commission assigns to effective records management, to outline key aims and objectives for the Commission in relation to its recordkeeping, and to provide the structure through which its records management policies, procedures and initiatives are to be delivered.

The Commission's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support business activity, policy formation and managerial decision-making; protect the interests of the organisation; and protect the rights of users of mental health, learning disability and social care services, which include

their carers and relatives. They support consistency, continuity, efficiency and productivity across the range of the Commission's activities.

Element 4: Business classification

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

The Commission has a business classification scheme (BCS). It is the intention that during 2014-15, the Commission will deploy the scheme we have produced in the folder structures of our IT systems to coincide with the move across to a planned new server. This classification scheme will also be adopted for use within the Commission Central repository, which houses final, approved version of corporate documents and is situated within IIMP.

An outline of our draft Business Classification Scheme is reproduced and can be viewed as **Appendix 3** of this document. **Appendix 4** is a letter from the Head of Corporate Services, endorsing this programme of work

Element 5: Retention schedules

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

The Commission is developing retention schedules alongside their Business Classification Scheme.

The Commission previously engaged an external consultant to examine this and other records management processes in the organisation, as a consequence of which a decision has been taken that our retention schedules would be incorporated into the Business Classification Scheme.

Operational areas within the Commission have been given a template to help them revisit the BCS and check and reclassify the information they create in a consistent manner and as part of this exercise they have also been asked to check existing retention periods and triggers and reset these as appropriate to align with current business need. Samples documents from this area of work are included as part of **Appendix 3.**

There remains work to be done to the draft BSC & retention schedules but we have established working groups and held meetings with representatives who are the folder "owners" or RM champions, from each functional group within the Commission. Representatives on these working groups have been the responsibility to facilitate the proper deployment of the schedules, and provide support to colleagues in implementing the schedules and retention schedules effectively.

These working groups have been meeting with the Information Manager and the VISIO diagrams and Excel spreadsheets contained in Appendix 3, provide evidence of the progress made following these meetings.

The Information Manager is overseeing this project and the mechanism for reporting progress will be via a newly established Records Management Review Group (RMRG).

The objective of the RMRG is to ensure that the Commission's records management plan is fully implemented. Moving forward, the RMRG will also be responsible for continued assessment and review of the records management plan.

This group will meet twice a year and its meetings will be incorporated into executive team meetings. Membership of the RMRG will comprise the executive team, and the Information Manager (IM). The group will be chaired by the Head of Corporate Services

The RMRG will provide a report annually to the Board.

The first meeting of RMRG will take place at 9.45am on Monday the 28th of July 2014.

(please see Element 13 for more details about the remit of the RMRG)

Element 6: Destruction Arrangements

The Commission has contracts in place for the bulk destruction of paper records and IT equipment containing electronic records.

Shred - it – Provides a confidential shredding service for paper records, company website: http://www.shredit.co.uk. This company provide the Commission with onsite secure bins, into which staff can discard confidential papers. Shred-it empty these bins on a regular basis.

Appendix 5 contains examples of certificates of destruction for paper records collected from the Commission as well as a copy of our contract with Shred-it.

CCL North Ltd – Provides a secure hardware destruction service for the Commission (to UK Government standards). The company website is: http://www.cclnorth.com/secure-data-destruction.html

Appendix 6 contains copies of documents certifying that Commission hardware has been destroyed in accordance with agreed standards.

Other evidence of our destruction arrangements are included in an amendment to the IT Security Policy – approved by the Commission's Operational Management Group in April 2014 **Appendix 7**

Evidence that this change to the policy have been ratified is evident from the minutes from the OMG meeting which took place on the 22nd of April. An extract of these minutes are available at **Appendix 8**.

Also included is a copy of the covering note that accompanied the proposed changes to the IT Security Policy when it was submitted to the meeting. **Appendix 9**

Finally there is a screen shot of our Symantec System Recover Log. **Appendix 10** This screenshot demonstrates that each back up wipes out any data previously stored on the drive and it is irrevocably destroyed and irretrievable.

Element 7: Archiving and transfer arrangement

This is the mechanism by which an authority transfers records of enduring value to an appropriate archive repository, specifying the timing of transfers and other terms and conditions.

In February 2014, the Information Manager met with Neil Miller and Leanne Jobling of NRS to discuss the review and update of the existing MOU between the NRS and the Commission. A way ahead was agreed and NRS provided the Commission with a template MOU. Following amendments by both organisations to the MOU, a final version is now ready for submission to OMG and, subject to any comment or change, it will then go to the September 2014 Board for final approval.

A copy of the draft MOU is available under **Appendix 11.**

Element 8: Information Security

Access to the Commission's offices is controlled by swipe cards, which are only issued to permanent and temporary staff. Access to the building's server room is by key pad, the combination of which is known only by the System Administrator and IT Support Officer. Individuals from other businesses who share the building may also access this server room but only where authorised to do so. Staff who access the server room require to have a specially modified swipe card and entry and exit to the server room is monitored. The temperature in the server room is maintained at a suitably low level, to safeguard server performance.

All new staff are provided with a copy of our IT Security Policy *(see **Appendix 7)*** and the IT Code of Conduct **Appendix 12** on entry. Staff **must** sign that they have read the IT Code of Conduct and agree to abide by its contents. The signed form is retained on their personal file, which is held by HR.

These policies are subject to regular review and update. New versions are published on the Intranet and set as a mandatory reads. HR can run reports and remind staff to read updated policies where they have not already done so.

The Commission's IT systems are password protected and a further password is required for entry to IIMP, which houses our electronic database.

Remote access to our IT systems is provided via encrypted laptop, which requires 2 factor authentication.

Passwords have built-in complexity and must be changed at set intervals, as prescribed in the IT Security Policy. Information across our IT systems is backed up to disk nightly, and each week the disk is taken off-site to be stored securely. The previous week's disk is brought back during this exchange.

The disks are transported in a secure, locked bag, the combination of the lock known only to the Systems Administrator, IT Support Officer and Administration Manager.

Related documents include the Data Protection Policy **Appendix 13** and the Information Risk Management Policy **Appendix 14**. Each of these documents is subject to periodic review.

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.

The Data Protection Act 1998 gives individuals the right to be advised of, and to request, copies of any personal data relating to them which is held by the Commission. Such applications are known as Subject Access Requests and are processed by the Commission in accordance with the Data Protection Act 1998.

The Commission holds a large volume of personal and sensitive information that is subject to the Data Protection Act 1998. This includes data on individuals with mental illness, learning disability and related conditions, which is also subject to the Caldicott principles. Other information we hold includes in relation to carers and relatives of those with mental illness, learning disability and related conditions; from other organisations such as NHS Boards, local authorities, Scottish Government, COPFS; on current, past and prospective employees; suppliers; and contractors.

The Commission is registered with the Information Commissioner's Office (ICO); registration entry is **Z9097121.**

The Commission has a Data Protection Policy, which sets out the approach taken by the Commission to data protection legislation.

The Commission has regard to Principle 7 of the Data Protection Act,
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

All computer systems at the Commission are password protected. IT staff manage access to different parts of the system and only those who require access as part of their jobs are given the necessary permission. A number of Commission staff, mainly practitioners, combine office based and remote working and all laptops used out of the office environment are double encrypted to a recognised European standard and in accordance with guidance issued by the Scottish Government and NHS Scotland

The Commission has also produced an "Information Risk Management Policy"**,** which highlights the potential risks, and associated implications, of accessing information out of the office and provides advice to staff about how to mitigate these risks

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 Commission's business continuity arrangements are embedded into its risk management processes. The Board has delegated responsibility for the overall risk management strategy and for ensuring it is incorporated into the business plan to the Audit Committee. The Risk Management Group meets twice yearly and at the second of these meetings, in late summer, the first three of the following documents are reviewed and updated:

- **Appendix 15** – Business Continuity Management (BCM) Policy
- **Appendix 16** – Vital Records – list of contents - USB key
- **Appendix 17** – The Covering letter to OMG to approve changes to the BCM Policy and the Vital Records paper
- **Appendix 18** - a note from the Head of Corporate Services endorsing the Commission's commitment to full implementation of this element of the plan.

These documents are presented annually to Operational Management Group (OMG) and, every 3 years, the BCM Policy is approved by OMG.

All records and data held by the Commission on its IT systems are backed up each night and, each Monday, because the Commission operates from a single building, the disk is taken to a secure off-site storage facility where it is exchanged for the previous week's disk.

Previously, the supplier of the Commission's bespoke IT system, IIMP, had stored a dedicated disaster recovery server under secure conditions and, annually, brought the server to the Commission to carry out a restore of the system from the back up disk. However, during 2013, the Commission assumed responsibility for its IT disaster recovery arrangements and carried out extensive testing to evidence our capability to restore our IT systems from the back up disk. The dedicated recovery server is now stored under secure conditions by Scottish Government. Disaster recovery testing is planned to take place at regular intervals.

As part of the disaster recovery arrangements, and because the Commission operates from a single site, information, including contact details, required in the event of a disaster is held on two encrypted USB keys which are retained off-site, one by the IT Security Officer and one by the Information Manager. Access to these keys would be essential in case a disaster occurs outwith normal office hours.

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.

The Commission does not have an Electronic Document and Records Management System (EDRMS) and it is unlikely that it will have resources to purchase and deploy such a system over the timeframe of this document. All information is processed electronically within our bespoke IT system, IIMP, and this system has a facility which allows us to track action that has been taken on forms, correspondence received and issued, telephone calls, and in relation to our visits and monitoring functions.

In addition to the above, when the Commission has fully implemented the new and approved Business Classification Scheme, staff will adopt agreed file naming protocols and method of version control. A draft copy of the Commission's file naming protocol is already available on the staff intranet along with other RM guidance documentation. **Appendix 19**

HR and Finance

The records held by both of these functions are stored within drives which are only accessible to the relevant staff. Disposal of records takes place in accordance with the timescales set out in the draft Business Classification Scheme.

Future planned developments

The Commission is committed to the development of a policy across the organisation that will promote the efficient management of records, which will involve adopting an established and universal hierarchical filing system and embracing good practice in naming conventions for files and folders. As part of this work we intend to transfer our electronic data to a new server, at which point we will create a clean structure in the network drives which will facilitate sharing, and avoid duplication, of files.

Element 12: Competency framework for records management staff

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

The Commission's size and budget does not allow it to have an individual post dedicated to records management. Instead, records management is included as a specific dimension in the job description of the Information Manager **Appendix 20** and is a key result area for the postholder. The Commission recognises that the Public Records (Scotland) Act 2011 places additional burdens on the organisation in relation to records management, which will need to be reflected in the role of the Information Manager. The Commission will look to identify resources to enable the Information Manager to receive training in the key concepts of records management. Staff will also receive training to ensure that they have an individual understanding of their records management responsibilities. Some work on the identification of key

competencies for all level of staff at the Commission was carried out by an external consultant and her findings are set out, in draft format, under **Appendix 21.**

In acknowledgement of our forthcoming obligations under the PRSA, the Commission contracted an external provider to look at our existing records management documentation and procedures during 2012. As part of this work, the contractor also delivered awareness-raising sessions with Commission staff (May 2013). These were mandatory, half-day sessions for all Commission staff. Copies of some of the guidance and an outline of the training programme can be found under **Appendix 22.**

The Information Manager does have responsibilities assigned to her under the organisation's Records Management Policy, including:

• develop and implement a records management plan.
• issue guidance and provide or facilitate training in records management to appropriate staff.
• support users of records management systems.
• ensure records management systems stay in line with developments in best practice.
• develop appropriate retention schedules and classification schemes.
• undertake compliance audits of records management programmes (policies, procedures and systems) to ensure Commission statutory obligations are met.
• develop strategies for the permanent preservation of selected records in conjunction with the National Records Scotland (NRS).

Element 13: Assessment and review

At the Operational Management Group meeting on Monday 16th June 2014 the group were asked to formally approve the establishment of the **Records Management Review Group (RMRG). Appendix 23**

The objective of the RMRG will be to ensure that the Commission's records management plan is fully implemented and that it delivers proper and effective arrangements for the management of all our records.

This group will meet twice a year. Membership of the RMRG will comprise the executive team, and the Information Manager (IM). The group will be chaired by the Head of Corporate Services

The RMRG will provide a report annually to the Board.

The proposed role and remit of the Records Management Review Group is as follows:

The group will ensure that a corporate approach to records management is adopted throughout the Commission.

It will review and, where appropriate, approve records management procedures and guidance published on the internet.

It will consider reports provided by the IM on progress towards implementation of the business classification scheme and retention schedules. These reports will be based on statements of compliance provided to the IM by each operational group - casework, corporate services and practitioner.

Role of the Information Manager

Besides preparing reports for the RMRG, the IM will prepare the agenda and take notes of these meetings. These notes will be made available to all staff via the Commission intranet

The first meeting of RMRG will take place on Monday the 28th of July 2014.

Element 14: Data sharing

Where data sharing takes place, it is carried out in line with the Data Protection Act 1998 and other relevant privacy information. Sharing of information is allowed only after an appropriate risk assessment has been carried out.

Registration with the ICO

Under Data Protection legislation, the Commission is required to register as a data controller with the Information Commissioner. This requires the Commission to stipulate, amongst other things, with whom it will or is likely to share data.

(see extract below of the Commission register entry, updated in July 2013)

Who the information may be shared with

We sometimes need to share the personal information we process with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act 1998 (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with, for one or more reasons.

Where necessary or required we share information with:

- data subjects *(service users, employees, suppliers, complainants or their representatives)*
- health and /or social work professionals and other service providers
- family, associates and representatives of the person whose personal data we are processing
- suppliers
- current, past or prospective employers;
- persons making an enquiry or complaint
- other ombudsman and regulatory authorities

MOUs/MOAs

The Commission has a number of agreements with other organisations. In most cases these agreements formalise, in a general sense, the data that can be and is shared between them on a regular and ongoing basis.

Copies of these agreements can be found on our website at;

Working with other organisations

Statutory sharing under DPA rules

Some data sharing carried out by the Commission is enshrined in legislation and is laid out in the Mental Health (Care and Treatment) (Scotland) Act 2003 and the Adults with Incapacity Act 2000.

Data sharing protocol forms

Occasionally, the Commission is asked to supply data not covered by either of the above. Where statistical data is not sufficient, requesters are required to complete a data sharing protocol form. A copy of this form is included under **Appendix 24.**

List of appendices

These documents are available to NRS to view but not all of them are in the public domain;

1. A letter from the Chief Executive of the Commission

2. Records Management Policy *(approved in January 2014).*

3. Business Classification Scheme (Excel spreadsheets and VISIO diagrams)

4. Statement of intent from Head of Corporate Services as regards elements Four, Five and Eleven.

5. Certificates of destruction for paper and a copy of our contract with Shred-it.

6. Copies of documents certifying that Commission hardware has been destroyed in accordance with agreed standards.

7. Copy (with notes of amendment) of the IT Security Policy – approved by the Commission's Operational Management Group in April 2014.

8. Extract from OMG minutes from 22nd April where changes to the IT Security Policy were approved.

9. A copy of the covering note that accompanied the proposed changes to the IT Security Policy when it was submitted to OMG.

10. Symantec System Recovery Log (screen shot)

11. A copy of the draft MOU between NRS and the Commission.

12. IT Code of Conduct

13. Data Protection Policy

14. Information Risk Management Policy

15. Business Continuity Management (BCM) Policy

16. Vital Records – list of contents - USB key

17. The Covering letter to OMG to approve changes to the BCM Policy and the Vital Records paper

18. A note from the Head of Corporate Services endorsing the Commission's commitment to full implementation of this element of the plan.

19. File naming protocol

20. Job description of the Information Manager

21. Key records management competencies for all level of staff at the Commission.

22. Records management awareness - training programme outline

23. Records Management Review Group (RMRG) - approval for the draft remit of the group.

24. Data sharing protocol forms
