Document and Records Management Policy

1. Introduction

1.1.   This document explains Ofgem's Records Management (RM) policy. It sets the framework within which all records must be maintained and operates at three levels, these are:

- **Overarching policy** (this document),

- **Procedures** :which sit beneath this policy and deal with the way in which particular aspects of records policy are applied,

- **Practices**: the day to day operation of the procedures, which exist usually in the form of operational manuals.

This policy sets the policy and tells the user where more detailed procedures and practices can be found.

2. Contacts

2.1.   This policy is the responsibility of the Research and Information Centre (RIC). Any questions about it should be addressed to;

- Paul Kitcher   -   library@ofgem.gov.uk   0207 901 7011

3. Background

3.1.   <u>All</u> Government Departments are required by statute to keep accurate records of their day to day operations.   Records are a key tool in ensuring that corporate knowledge is managed, that the right information is retained, and that out of date or redundant information is disposed of when no longer needed.   Appropriate management of records has a direct impact on the day to day operation of the department, and the quality of records directly influences Ofgem's ability to regulate the energy industry.

3.2.   Records form an audit trail of decisions made by Ofgem. They can be hard copy (paper), on video or CD, or stored in the Ofgem Electronic Document and Records Management system (ERDM) in the Microsoft SharePoint environment, this system is divided into two working areas the documents management (site and library areas), and the Records Area (sometimes referred to as the Registry). Unless there are substantive reasons for doing otherwise from April 2008 the main location for storing Ofgem's records is the Registry.   Exceptions are noted in section [7].

3.3.   The actual responsibility for record keeping in the organisation is Ofgem's Accounting Officer.   This reflects Parliament's view that Ofgem's records are vitally important to the management of the organisation.

3.4.   Authority to manage records within the department is delegated to the Departmental Records Officer (DRO) who is responsible for the day to day running of the records function in Ofgem. Ofgem in common with all Government Departments operates a Registry which tracks the location and status of hard copy records and manages the SharePoint function within the RIC.   RIC operates within the Information

Management and Technology team who also have responsibility for the I.T. environment where many records are now created.

3.5.   Ofgem's RM policy is also instructed by third parties, usually Other Government Departments (OGDs), who set the legislative framework for RM. The main Departments involved are;

- the Cabinet Office - setting national policy on most Government administrative policies from records management though to security

- the Ministry of Justice (MOJ) - setting national standards for RM though The National Archives (TNA).   TNA instructs all government departments in the way in which records are managed.   This can result in changes to policies and operational procedures which Ofgem is obliged to apply.

3.6.   The legal framework includes (but is not limited to) all of the following UK legislation;

- Public Records Acts 1958 & 1967 (PRA)

- Freedom of Information Act (section 46) (FOI)

- Data Protection Act 1998 (DPA)

- Gas Act 1986 (GA)

- Electricity Act 1990 (ELA)

- Utilities Act 2000 (UA)

- Enterprise Act 2002 (EA)

- Energy Act 2004 (ENA)

- Official Secrets Acts 1911 and 1989 (OSA)

European Union (EU) law also applies.

4. Policies and Procedures and Practices

4.1.   **Policies** - The RM policy works in tandem with a number of other policies and procedures in place within Ofgem, for example records retention policy and security policy.

4.2.   **Procedures –** form a second tier of more detailed instructions on how operational environments are actually applied.   The two main procedures related to this policy are:

- SharePoint management procedures

- Paper File and Archive management procedures

4.3   **Practices –** are instructions that are used for day to day operations, usually manuals.   In a SharePoint context manuals have been written to enable users to operate within the environment. SharePoint manuals can be found in the internal RIC website. Other manuals which instruct users on how to produce records in other Ofgem IT environments are listed in their own procedures and practices documents.

5. Documents, Records and Record Lifecycles, Record organisation

5.1   It is important to realise that there is a difference between a document and a Record.   A document is a piece of information usually in written form that Ofgem has produced or received. It will usually be stored electronically within a SharePoint or occasionally in hard copy. A document is usually either work in progress, or something that is not needed long term (ephemeral in RM terms).   A sub set of documents that are SharePoint in will become records.   Not all documents are records, but many records are documents.

5.2   A record is created (or received) and maintained as evidence by an organisation, person or business to ensure that their legal obligations are met. Records are products of business being conducted by that organisation so are usually produced in support of or to enable business processes.

5.3   For Ofgem records can be a simple as the agreement to purchase stationary and the subsequent financial transaction that takes place to complete that purchase, or as complex as a full price control where a lot of data is collected, analysed, and used to make policy decisions that affect major companies operating in the UK energy market.

5.4   Both documents and records and are stored within the SharePoint and are organised in `libraries', essentially collections of folders.  Several libraries can be collected together into groups called `sites'.   Libraries are managed by staff across the organisation called Local Knowledge Managers (LKMs), who are involved in the day to day management of both the document area. The LKM framework sets out LKM duties.

5.5   Paper records are simply hard copies of documents. They, like their electronic counterparts are not confined to material generated within Ofgem, for example invoices or responses to consultations are just as much records regardless of whether they are hard copy or electronic.   Similar conventions apply to the management of paper files as apply to electronic ones.

5.6   Records have a formal lifecycle, each stage of which is supported by its own, policies and procedures. The simple version of the lifecycle of a record is;

- **Creation** – usually the writing or importing (to SharePoint) of a document and storing to a permanent form in the Records Centre

- **Active Records** – records that are referred to regularly and are being updated or added to from time to time

- **Dormant Records** – These are records where the actual activity has been completed.   When the last action on the record set is completed the records are closed and a review workflow started (see retention policy for more detail), this reminds the owner to look at the information again to decide if it is still needed.

- **Records Removal** – This is the last stage of a records life removing it from the system whether paper or electronic. Removed files are either destroyed or deleted, or if of historical interest can be transferred to TNA for more public use.

6. Who is Responsible for Managing Records?

6.1   The short answer to the question is everyone.   Records are managed by five tiers of staff, each of who have slightly different access rights within both the electronic and paper RM systems. The levels of responsibility are set out in the table below. In addition some I.T staff have administrator rights which allow permissions such as read, and write to be limited within certain libraries.   Administration rights are set by I.T. policy, and are set out in ECM procedures.

Staff Title (Abbreviation)	Role	Notes
IT Staff	Management of users access rights, code, backup and maintenance of EDRM system	IT staff must not be implement structural or rights changes without an approved business cases signed off by the DRO and head of IT.
Research and information Centre (RIC) staff	Management of overall structure of ECM, including the setting up and reviewing folder library and site structures. Responsible for the setting up of paper files where required, and recording their location and status. Management of paper archive. RIC staff are also responsible for records management training, both in the ECM and paper environment.	Only staff able to delete files from the SharePoint Records / Registry area or recall paper files from archive, or destroy paper files. Day to day contacts for RM policy. Advisers on records security. RIC staff only have day to day read `rights' within libraries that are open' or where they specifically need access RIC does not for example have access to the HR work area (and many others).
Local Knowledge Managers (LKMs)	Agree and manage file plans within local ECM libraries, move documents to storage areas.	Responsible for the review of electronic records when they reach the end of their useful life (retention reviews). LKMs will usually have access to all areas of the libraries which they manage.
Content Authors (CAs)	Responsible for the development of documents to the stage where they are able to be published to the Ofgem website or Intranet. All documents that are published must be saved to the Records/Registry on the system.	LKMs can also be Content Authors.
Users	All staff have the responsibility for saving documents that are important to Ofgem as part of the decision audit trail into the Registry /Records area of the ECM system, as well as the development and download of working documents into the document system.	Users who do not have LKM rights do not have rights to set up folders in the ECM system. May request set up of paper files or recall paper files from archive.

6.4   In most cases staff from one tier of the network management will have rights to the layers below, though not all RIC and LKMs staff have CA rights.   All Ofgem staff have user rights, though many may have unique access to some parts of the SharePoint system; HR for example are the only ones who have access to their own work areas.   Access rights are managed though permissions which are set out in the procedures documents.

7. How Documents and Records are managed

7.1.   Ofgem needs to manage its documents (work in progress), and records (audit trails of decisions) in accordance with UK and EU law. We also need to make the most effective use of the information resource that the ECM system (and paper records) hold. To enable this there are a few basic principles that apply, these are set out in

brief in this section of the policy, and in more detail in the SharePoint Procedures document.

7.2.   Managing Libraries

7.2.1. Within the ECM system the main management unit for documents is the library. The number of libraries will vary, as will their contents.   The general principles that apply to libraries are as follows;

- libraries are repositories of work in progress, they are <u>not</u> records in their own right

- libraries may be one of three types; Open, Closed or Hybrid (partially open)

- open libraries are viewable and editable by all staff. Unless there is a substantial business reason to do otherwise all libraries are Open

- closed libraries are where access is limited to very few staff; business cases for closed libraries must be signed off by the Director for that area, and referred to RIC for approval.   RIC may refer the case to SMT for confirmation.

- hybrid libraries where some parts of the folder tree are protected by permissions are also permitted. Theyare preferred to closed libraries.   Again business reasons to restrict those parts of the library must be submitted to RIC.

- no SharePoint library should contain information marked by Ofgem as `Confidential', `Secret`, or `Top Secret'.   The Ofgem network is not sufficiently secure to contain such information.   Read the Security Manual or seek advice from RIC on how information at that level needs to be processed

- Information received from this parties marked as `Confidential' should be reassessed as set out in the security manual.  Most will be marked as `restricted' or 'protect'.

7.3.   Managing documents

7.3.1 Documents are individual works in progress held in individual libraries. Documents are distinguished from records in that they are not yet regarded as important enough or complete enough to be saved as a record, and therefore be transferred into permanent storage.

7.3.2   The following principles apply to all documents in SharePoint

- All documents must be of a defined content type.   The content type determines what information is needed to distinguish a document or record

- documents may be of <u>any </u>file format that is supported by Ofgem's I.T. system and can be saved on SharePoint

- key data about documents (such as the date created, version, and type of document, author and recipient) must be recorded in every document.   This is referred to as `metadata'. Documents cannot be checked into the system without metadata

- documents <u>must</u> be `checked in' when not in use to ensure the widest possible availability of information to all staff (checked out files are not visible to non LKM staff)

- documents <u>must not</u> be password protected – sensitive data is managed by permissions set up by I.T. within a hybrid library

7.4. Records and the Records Centre

7.4.1. Records on SharePoint are those documents that are regarded as important enough to save in a permanent form.   To do this they are saved into a second SharePoint location, the Records Centre, usually referred to as the `SharePoint Registry'. Documents saved into this area can only be deleted by direct intervention of the RIC team.   The principles governing the records are:

- the electronic Records Centre is open to all staff to view records that are saved in this area

- all documents that are required as part of an audit trail of decisions must be saved as records

- final versions of documents must be saved as records (including externally generated documents

- all documents sent to the Ofgem web site <u>must</u> be saved as a record

- only RIC staff have rights to delete records in the Records Centre

7.4.2. A retention review `workflow' document must be sent to the records area when a piece of work (usually many documents converted to records) is complete.   This prompts the RIC to review a record set when it is no longer likely to be of further use. As a result it may be archived or destroyed.

7.5. Staff Responsibilities

7.5.1. The next few bullet points cover <u>who</u> is responsible for doing what;

- RIC is responsible for the setting up of SharePoint Sites and Libraries and for management of the electronic records area.

- LKMs are responsible for requesting new libraries and Sites from RIC, including their security settings

- LKMs are responsible for the internal folder structure of libraries, and for setting retention reviews on groups of documents sent to the library.

- LKMs are also responsible for enforcing the check in of documents in their libraries. Checking in ensures that documents are available as widely as possible for collaborative use.

- CAs are responsible for publishing documents from libraries to the Ofgem website and intranet, whenever they do so they <u>must</u> save a copy of that document to the registry

- Users produce and edit documents within libraries. They should also send documents that need to be kept long term from the document management are to the registry

- Users must not send personal data to the Registry, all data sent to the registry is visible to all staff and it is very likely that Ofgem would be in contravention of several principles of the Data Protection Act, particularly section 10 should we store personal information in the registry when it is not needed.

7.5.2. <u>Information must be removed from the system if</u>*:*

- The document's security status is `confidential', `secret' or `top secret' in which case it must be stored securely <u>off system</u>.

- It is personal information (within a closed library) and needs to be stored as a record. The record must go to a secure repository such as TRENT or CRM.

7.5.3. The need to store confidential, secret or top secret information must also be notified to RIC so that suitable storage arrangements can be made and the Confidential Information Register (CIR) kept up to date with the location and owner of the information*.*

7.6.   Managing Paper Files

7.6.1. It is policy to store newly produced documents and records as far as possible on the SharePoint system. However, there are some instances where this is not possible, e.g. for Security, Data Protection or legal reasons. Many of these records will need to be maintained in paper form.   Ofgem's Registry located in RIC sets up, archives and reviews paper files. The current location and status of all files (including those that have been destroyed) is recorded in the Registry Database.

7.6.2.   Ofgem already has registered (recorded on the registry database) over 75,000 paper files. Despite the existence of the SharePoint system it is a legal requirement for us to manage these until;

- they are no longer needed and are either destroyed or sent to TNA

- the law changes

- their security status falls below `confidential'

- they are scanned onto the system and they are no longer needed.

7.6.3. Although it is permitted to scan files on to the ECM system it is <u>not</u> policy to do so, due to the volume of files that exist.   Should a decision be made to scan a paper file into the system it is saved into the Registry area, the file can be destroyed, provided it is not in one of the categories in paragraph 7.6.4 below.

7.6.4. The following <u>must</u> be retained in paper format;

- Any information ranked as `Confidential` or higher this information <u>may not</u> be scanned into the ECM system.

- Any personal information that is needed on site, and cannot be accommodated in stand alone systems such as TRENT or CRM

- Any documents that have formal `legal` signatures on them such as licences, determinations or contracts.   (Electronic versions of these should also be placed on the ECM system).

- All documents that are part of the public register. These need to be available for public viewing in the RIC, in accordance with the Gas Act, Electricity Act and Utilities Act.

7.6.5. Staff may also decide that a file of hard copy papers is required for quick reference, particularly where papers are needed for meetings. In many cases these files may only exist for a day or two, in which case they do not need to be registered.   If however, the file is needed for an extended period, it is good practice to register the file, even if it duplicates electronic information. Temporary registered files can be destroyed as soon as they are no longer required.

7.6.6. Any paper files that are required need to be set up and formally recorded by registry.   When a file's status changes (e.g. if it needs to be closed or a new part needs to be set up), Registry is where this process occurs.

7.6.7. When a file is no longer needed for day to day reference it is `put away' or archived off site.   Registry manage access to off site storage.   Retrieval of files is next working day, provided that the order is placed before 2.30 pm.

7.6.8. The paper archive is in general accessible to all staff, though there are restrictions on what can be requested.   These restrictions follow patterns of what may be viewed by staff on the SharePoint system, for example only HR may retrieve HR files.

7.6.9. Paper files are subject to review in exactly the same way as electronic files. Due to the volume currently owned by Ofgem it is policy that files are only formally reviewed when sent to or retrieved from archive. There are four possible outcomes of a review;

- Destroy

- Retain for further review (usually send back to archive)

- Refer to TNA (i.e. release from Ofgem control)

- The file is `reactivated'

8. Security

8.1.   Ofgem's security policy is available on the intranet.   It distils policy from the Cabinet Office `Security Policy Framework' into a an Ofgem context It includes several sections, which apply to RM policy.   These are;

- Clear desk policy

- Document Security

- IT policy (use of system)

- Document Security Marking

8.2.   Ofgem staff are required to operate within these security limits.

9. Email Policy

9.1.   Email is a key system that generates a significant numbers of records. It has its own policy which covers terms of use, including further guidance on what should be saved as a record.

10.   Retention Policy

10.1. TNA sets the framework for retention policies at national level.   The retention policy sets out how long a record needs to be held before it is reviewed archived or destroyed.   Paper files are managed by RIC in the same way as files on SharePoint.

10.2.   Most Ofgem records have a useful shelf life of between one and seven years, though in many cases we may keep information longer, up to thirty years in some cases.   In Ofgem's case many policy records have to be destroyed at the end of their useful life as provisions within some of our governing legislation (e.g. section 105 of the Utilities Act).

10.3.   Retention policy is enabled by retention review documents stored in the records centre when record sets are complete. These start workflows that tell RIC to review files after three, five or seven years.   Most files with 3 or 7 year retention schedules are destroyed at first review.   Files with 5 year reviews may be destroyed, retained for a further review or, if no longer needed and of public interest sent to TNA.

11.   Information Rights

11.1.   RM policy has to operate within the context of the Information Rights Policies. This covers the:

- Data protection Act 1998

- Freedom of Information Act 2000

- Environmental Information Regulations 2004

- Re-use of Public Sector Information Regulations 2005

11.2   It is our obligation under S46 of FOIA to maintain a complete record, and identify where documents requested are, failure to do so may result in a formal audit by TNA.

12.   Managing other Data and Record Repositories

12.1.1.   There are a number of other record repositories outside of the formal paper and ECM system.   The main ones are;

- Finance System (Sun Accounts)   Owner : Head of Finance

- Environmental Programmes System   Owner : Head of Environmental Programmes
  (EPS)

- Customer Relationship Management   Owner : Head of Consumer Affairs
  system (CRM)

- HR System (TRENT)   Owner : Head of HR

- Building Access and CCTV system   Owner : Head of Building Services

Each of these systems is stand alone and data on them is only available to staff employed in that team and is entirely controlled by Ofgem staff or contractors employed by Ofgem.   Access to these systems is managed by the system owner.

12.1.2.   Some information may be transferred between Ofgem systems, for example some HR information may be transferred from ECM document libraries to and from TRENT, or between TRENT and Sun.   Each system has its own operating instructions and is compliant with Ofgem retention policy, for data and records contained within it. Responsibility for day to day compliance with those policies rests with the individual system owners.

13.   Further Reading

13.1.   This policy is necessarily broad brush as it deals with records and documents stored both electronically and in hard copy.   Secondary policies and procedures deal with some issues in more detail.   You should refer to the following:

- **SharePoint Procedures**; this sets out how SharePoint rights are assigned and what users (and in particular LKMs) need to do to ensure that there is appropriate level of access to systems

- **Retention Policies:** this sets out how long records (whether electronic or paper) need to be held.   This document is applicable beyond the SharePoint

- **Information Rights:** deals with the implementation of the four information rights Acts. This document is applicable beyond the SharePoint system.

- **Security Policy:** Sets out I.T. and document security policy as well as physical security information.   This document is applicable beyond the SharePoint system.

Ofgem RIC

March 2009