date – 5th September 2019

Trust in water

ICT8 Information and Records Management Policy

www.ofwat.gov.uk

Ofwat

Table of Contents

1. Introduction

Information is the lifeblood of any organisation – essential to the delivery of high quality evidence based programme and project delivery and administrative support functions on a day to day basis.

The Chief Executive and Senior Information Risk Owner (SIRO) are accountable for information and records management therefore they should ensure that it corporately meets its legal responsibilities by providing appropriate mechanisms to support the Information and Records Management team, delivery and continuity.

Ofwat will conform to a number of legislative requirements, regulations and standards that are particularly relevant to their management of records and these are detailed in section 5 of this policy.

Implementing best practice in records management throughout Ofwat means that “A systematic and planned approach is in place for the management of records, from the moment a record is created until its ultimate disposal, that the organisation can control both the quality and quantity of information it generates; can maintain that information in a manner that effectively services its needs and those of its stakeholders; and it can dispose of the information appropriately when it is no longer required”.

By law records must be managed properly. The following statutes set out the specific requirements for the creation, management and disposal of records:

- Data Protection Act 2018,
- The Freedom of Information Act 2000 (particularly Section 46: Lord Chancellor’s Code of Practice on records Management)
- The Environmental Information Regulations 2004

The following standards provide the necessary framework for the effective and efficient document and records management and represent records management best practice:

- ISO 15489 – Records Management Standard
- ISO 27001 – Information Security
- BS 10008 Evidential weight and legal admissibility of electronic information

For the purpose of this policy, a record is 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.” (BS ISO 15489.1)

The principal issues for the management of electronic records are the same as those for the management of any record. They include, for example the creation of authentic records, the tracking of records and disposal arrangements. However, the means by which these issues are addressed in the electronic environment may be different.

2. Purpose

The overall aim of this policy is to contribute to the achievement of Ofwat’s Vision, Mission, Values and Strategic Objectives by improving and promoting the effective management and use of information. This means recognising the value and importance of information as a corporate resource for the delivery of corporate and service objectives in order to deliver a professional and excellent service to stakeholders.

The policy will facilitate the communication to all Ofwat people of their roles and responsibilities in maintaining legal compliance and best practice when recordkeeping.

The purpose of managing records through the stages of a ‘Lifecycle’ is to set out the arrangements for:

- Managing the risks associated with the quality of records in all formats by providing a framework and standards for practice

- Managing the risks associated with records in all formats by establishing and embedding systems to properly control records throughout their lifecycle
- To comply with legislation.
- To ensure that the security and confidentiality of records are maintained.

3. Scope of the policy

This policy covers all information held and processed by Ofwat. It sets out the strategic governance arrangements for all information created and received in accordance with agreed best practice, principles, statutory and mandatory requirements as in section 5 of this policy.

This policy is mandatory and applies to all information in all formats through all stages of an information lifecycle from creation through to disposal.

This policy will apply to:

- All people working for or on behalf of Ofwat, including full-time, part-time, non-executive directors, contracted third parties, agency staff, students, trainees, secondees, staff of partner organisations with approved access, visiting professionals, researchers, volunteers and companies providing other services to Ofwat e.g. IT
- All documents and records held, used or managed by Ofwat regardless of their media,
- All IT application systems within Ofwat including databases, information systems and registers,
- Any records held, maintained and managed by third parties under contract to Ofwat,
- Any records transferred or supplied to Ofwat unless more stringent terms and conditions of use and/or management are identified and agreed in separate service level agreements, identifying ownership and rights of the information supplied.

4. Responsibilities

Chief Executive has overall accountability and responsibility for information and records management and this function is delegated to the SIRO, who is responsible for driving forward the achievement of improvements identified in this policy

Senior Information Risk Officer (SIRO) is responsible for reporting to the Board all aspects of information risk. This will include any risks relating to records or data. These risks will be identified, assessed and reported using the established organisational risk management process and overseen by the Security and Information Assurance Group (SIAG). The SIRO is supported by the Information Governance Manager

Information Governance Manager (IGM) is responsible for information and records management. They will also manage inactive records in both paper and electronic formats. The Information Governance Manager will:

- Lead and support the development and maintenance of information and records management policies, procedures and practices, in particular for providing advice and guidance for good records management practice and promoting compliance with this policy to ensure the effective, efficient and appropriate retrieval of information.

- Be responsible for advising and training staff on archiving, retrieval and permanent preservation of records.

- Monitor compliance with records management legislation, standards, policies, procedures and best practice

Deputy Security Advisor (DSA)
The Deputy Security Advisor is responsible for the management and strategic development of cyber and physical security including the allocation of security duties, and is the first point of escalation for security issues.

Information Asset Owners (IAOs)
IAOs are responsible for identifying, understanding, managing, reporting and recording risks in relation to their Information assets. They also have a role in leading and fostering a culture that values, protects and uses information for the benefit of Ofwat and our wider stakeholders.

Information Asset Co-ordinators (IACs)
An IAC is someone who has been delegated to look after the day to day activity and to support the IAO

All Ofwat people are responsible for any records which they create or use. This responsibility is established at, and defined by, the Public Records Act 1958. As an employee of the Civil Service, any records created by an employee are public records. Individuals are also responsible for adherence to national, local and Ofwat's own defined record keeping and record management policies. All employees are responsible for documenting their actions and for maintaining records in accordance with good records management practice and professional guidelines.

5. Procedure and Implementation

All employees must be aware of their obligations and the requirements surrounding compliance with the complete lifecycle of a record. All employees must ensure that records:

- Contain the information required in order to reconstruct activities or transactions that have taken place (The record must include who, what, where, when, why and how),
- Can be easily located and accessed if authorised to do so, by use of appropriate software and hardware, and displayed in a way consistent with initial use,
- Can be interpreted so that the context of the record i.e. creator, the business process and the relationship to other records is apparent,

- Can be trusted and are accurate to ensure integrity, authenticity and reliability,
- Can be maintained through time so that accessibility, interpretation and trustworthiness remain throughout the records lifecycle despite migration between hardware, software or digital media.

Once declared, a **record** must not be changed or modified in any way.

All electronic records must contain sufficient metadata (descriptive and technical documentation) to enable the system, and the documents and records it contains, to be understood and operated efficiently, and to provide an administrative context for the effective management of the documents and records.

Electronic documents and records must have sufficient metadata applied to them to enable them to be properly classified, stored and retrieved.

Prior to assigning any sensitive or confidential information to a storage location (including offsite storage), it is imperative that the information is marked appropriately. Protective markings must be applied wherever possible to all filing systems for documents and records regardless of the media on which those documents and records are held. This is to ensure that all documents and records are managed according to the same principles, and that all holdings on any given subject can be accounted for.

The movement and location of all documents and records must be controlled to ensure that they can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions. The electronic transmission of official and/or confidential information must adhere to the principles set out in the Handling Sensitive Information guidance available on the Source.

Documents and records must be protected from inappropriate access, alteration, misinterpretation and loss. Access to official or confidential documents and records will be on a “need to know” basis and all access rights are subject to formal authorisation whether internal or from external parties.

Documents and records must be maintained to ensure that the content, context and structure are accessible, comprehensible and managed for as long as record keeping requirements determine, without loss of information.

Records must be disposed of or transferred as appropriate in line with Retention and Disposal Policy.

Vital records must be identified on the information asset register by being flagged as key assets, stored and maintained in line with the guidelines set out by the National Archives. These will be subject to more rigorous maintenance schedules than standard records. Vital records are defined as: “Those records which are essential to the continued operation of the organisation and which are irreplaceable” (McKinnon, G, 1977)

The appraisal of records and documentation of their disposal must be undertaken regularly in line with the Retention and Disposal Policy

Documents judged not to be records must be disposed of appropriately as soon as they cease to be active.

In respect of any documents that contain personal data, the storage limitation principle of the General Data Protection Regulations 2016 applies, i.e. that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed' '

The importance of a record, and as such its appropriate retention period, may change over time and as a transaction or project progresses. Appraisal decisions are informed by the functions of the organisation and by assessing both Primary and Secondary values.

Primary value is the business transaction that gave rise to the creation of the record which includes:

- Operational/Administrative
- Financial/Fiscal
- Legal

Secondary value is the purpose other than the business transaction for which the record was created and includes:

- Informational – reference, research
- Intrinsic – historical, physical form/features, aesthetic/artistic quality
- Monetary value

The power to allocate retention and disposal schedules to specific records will rest with the Information Governance Manager and any other staff who the Information Governance Manager deems appropriate to delegate this responsibility to. A schedule will be allocated upon the creation of a record, and can be changed by request at a later date in line with the Retention and Disposal Policy.

Records are required to be kept for a certain period either because of statutory requirements or because they may be needed for administrative purposes during this time. This is a **minimum retention period**.

The retention and disposal policy includes a schedule which states:

- A triggering event, such as the review date or closure of a record
- A retention period, such as 6 years
- Disposal actions, such as review, export, transfer, or destroy

Records will be closed as soon as they have ceased to be of active use other than for reference purposes. Wherever possible, information on the intended disposal of electronic records must be included in the metadata when the record is created or declared as a record i.e. closed or changed to 'Read Only' or converted to PDF.

The storage of closed physical records awaiting disposal will follow accepted standards relating to environment, security and physical organisation.

The location of official/or confidential information for review and audit purposes must be properly recorded, it will create and maintain a centrally-based register of physical storage repositories and electronic storage repositories both on-site and off-site.

Equipment and storage facilities used for records must provide storage which is safe from unauthorised access, meets fire regulations, provides an inventory of all records held, provides an audit trail for the tracking of records and also allows maximum and timely accessibility to the information commensurate with its frequency of use.

Physical records no longer required for the conduct of current business, will be placed in an appropriate storage repository rather than in office accommodation.

Audit trails will be provided for all electronic records and documents. They will be kept securely and will be available for inspection by authorised personnel.

All scanned records where the original master was once born physical and the master has transferred to the electronic copy will conform to the provisions of BS10008 - *Evidential weight and legal admissibility of electronic information* especially for those records likely to be required as evidence.

Records identified by staff as being suitable for permanent preservation (whatever format) no longer in regular use and not published on the Ofwat website and therefore captured by the web archive process, must be reported to the Information Governance Manager, who will liaise with the National Archives to arrange transfer of said records, subject to the approval of the National Archives. Records not selected for permanent preservation and which have reached the end of their administrative life will be destroyed in as secure a manner as is necessary for the level of confidentiality or security markings they bear.

It is particularly important under Freedom of Information, Environmental Information Regulations and Data Protection legislation that the disposal of records - which is defined as the point in their lifecycle when they are either transferred to archives or destroyed - is undertaken in accordance with clearly established procedures which have been formally adopted and which are enforced by properly authorised staff.

If a record due for destruction is known to be the subject of a request for information, destruction will be delayed until disclosure has taken place or, if it has been decided not to disclose the information, until the complaint and appeal provisions of the FOI Act have been exhausted.

Records may only be disposed of in accordance with established procedures and time-scales identified in Retention and Disposal Policy. A record must be kept of the destruction of all records, which enables an identification of the record to be made, and includes documentation of the record’s destruction, including date and authorisation for the disposal actions. Similar details must be kept on the destruction of all physical records, and a “Certificate of Destruction” obtained for any records destroyed by an outside company.

Electronic records that are no longer required for business purposes must be capable of being deleted/destroyed in such a way that they cannot be recreated. This must be considered if using a database e.g. Microsoft Access which cannot be deleted from.

All records must be accounted for and incorporated into the Business Continuity Plan (BCP) as required by ISO 15489.

A back-up regime is detailed in the IT Disaster Response Plan.

After the back-up process, any records created, modified, destroyed or transferred will be reinstated and therefore staff must be aware that records will have been lost during a specific time period and records which were deleted will also be restored. Anything that is sent via email will have been received by the recipient however; the master copy will not be available. Recipients should be contacted to gain a copy of this email if required.

6. Training Implications

All new staff will be made aware of the existence of this policy via the induction process and a copy will be available on the Information and Security area of the Source. Resource Managers must highlight to staff their responsibility to ensure that they review the content of this policy and the importance placed on the appropriate creation, management, retention and disposal of records.

Resource Managers must actively ensure that all staff who create, manage, transfer, retain or dispose of records undertakes appropriate training opportunities.

Training will be appropriate to the individual employee's role, regularly assessed and refreshed so that employees remain appropriately skilled and knowledgeable over time.

The Information Governance Manager will develop, maintain and publicise promotional material to raise awareness of records management.

7. Monitoring Arrangements

Area for Monitoring	How	Who by	Reported to	Frequency
Policy	Review of best practice against the policy will be undertaken annually through auditing	Information Governance Manager	SIAG	Annually

8. Links to Any Associated Documents

ICT 2 Security Policy
ICT 4 Retention and Disposal Policy
ICT 5 Information and Technology Security Policy
ICT 6 Acceptable Use Agreement
IT Disaster Response Plan
Government Classification Policy
Handling Market Sensitive Information Guidance
Ofwat Code of Conduct
G1 Access to Information Policy
G2 Data Protection Policy
G3 Freedom of Information Policy
G5 Privacy Policy

9. Document control

Version history

Version	Date	Author	Changes to previous document
0.1	05/10/2015	Record Manager	First draft for review
0.2	06/10/2015	Record Manager	Minor amendments
0.3	27/04/2016	Record Manager	Amendments from Rebekah Eden and Simon Smith following SIAG consultation.
0.4	29/06/2016	Record Manager	Change from Policy to Policy and Procedure.
1.0	02/09/2019	IGM	Legislation and Procedural updates

Sign off

Job Title	Date	Version No.	Date of Next review
DPO	Sept 2019	1.0	Sept 2021