



Records Management Standards for the BBC

DQ Status	BBC Standard		
DQ Content Authority	Steve Jupe, Intake Media Manager		
Contact(s) for Help	Steve Jupe		
Description	<p>The records management standards for the BBC have been devised to ensure that records are created and maintained to a level necessary to safeguard the interests of the corporation. These standards have been written in accordance with the BBC's Core Records Policy. Adherence to the standards will assist compliance with the policy. Failure to comply could result in the BBC suffering legal action, damage to its reputation, financial losses, or the diminishing of its heritage</p> <p>The standards apply equally to paper records and to records created, stored, or captured by an electronic system.</p>		
DQ Reference	Version	Date	Last Reviewed
I&a_20_02	01.02	27/10/2008	27/10/2008
Who reviewed	Nick Watson, Iain Gibson, Julia Harris, Jacque Kavanagh		
Key Words	Records, management		

Please ensure you are using the current version of the document which is located:-

on gateway :-

http://guidelines.gateway.bbc.co.uk/dq/media_management/records_management.shtml

on bbc.co.uk :- will be available on <http://www.bbc.co.uk/guidelines/dq/contents/archives.shtml>

Contents

INTRODUCTION	3
MANAGING RECORDS IN THE BBC	4
Introduction	4
Legal Admissibility	4
Personal information	4
Retention scheduling	5
Secure storage	6
Access and retrieval	6
Meaningful Context	6
MANAGING ELECTRONIC RECORDS	7
Introduction	7
Electronic Records Management Systems	7
Record Integrity	7
Security and Access	7
Protection	8
Migration	8
Integration with paper-systems	8
Scanning	8
Shared Folders and Email	9
RECORD SECURITY	10
Introduction	10
Physical Security	10
Electronic Record Keeping Systems	10
Access Control	10
Record tracking	11
Integrity of Records	11
METADATA REQUIREMENTS	12
Required Metadata Elements	12
STORAGE REQUIREMENTS	14
Digital Storage	14
Physical Storage Units	14
Protection of Paper Records	15
Microfilm	15
RECORD TYPES	16
Definitions	16

Introduction

The records management standards for the BBC have been devised to ensure that records are created and maintained to a level necessary to safeguard the interests of the corporation. These standards have been written in accordance with the BBC's Core Records Policy. Adherence to the standards will assist compliance with the policy. Failure to comply could result in the BBC suffering legal action, damage to its reputation, financial losses, or the diminishing of its heritage.

Records covered by these standards are those created or received by BBC employees during the undertaking of their duties. All records created are the property of the BBC as a whole, and not that of the creator or an individual department. Responsibility for ensuring that records adhere to these standards rests with both the creators and custodians.

The standards apply equally to paper records and to records created, stored, or captured by an electronic system. Additional requirements are placed on the management of electronic records, necessitated by the more complex environment.

See also:

BBC Records Management Policy -

http://guidelines.gateway.bbc.co.uk/dq/media_management/records_management.shtml

BBC Information Security Policies -

<http://guidelines.gateway.bbc.co.uk/dq/is/policies.shtml>

Managing Records in the BBC

Introduction

Records must be created where determined by legal or business requirements; they must contain adequate information for legal, legislative, business and administrative needs.

Where there is a need to document a transaction to satisfy legal requirements, or to inform future business, accurate records must be created and maintained. The protection of the BBC from any future litigation or business losses is vital. Creating full and accurate records will ensure that evidence is available and that business processes and policies are recorded for future use by either the issuing office, or another BBC department.

The responsibility for the creation of these records falls on the department undertaking the transaction. The information contained within the records must accurately reflect the action, communication, or decision being recorded.

Legal Admissibility

For records to be legally admissible it may be necessary to prove that the information contained within them is accurate, complete and has not been altered. Any system in which records are stored must be trustworthy. Secure procedures for the capture and storage of documents into a record-keeping system must be created. It must not be possible to alter, or wrongly destroy, a record that has been entered into a record-keeping system.

The authentication of records will be required when producing them as evidence in legal proceedings. The legal weight of records will be greater if the original version is produced. Where the original cannot be produced, it is important to prove that any copies are accurate reproductions of the original.

Personal information

Records containing personal information must comply with the Data Protection Act. Guidance on the act can be obtained from the BBC's Information Policy & Compliance Team.

Retention scheduling

BBC offices have a duty to hold records for specified amounts of time to meet administrative and legal needs. Legislation also places requirements on the retention of records. Certain records must be held for a minimum period (e.g. financial information), while others must only be held as long as needed (e.g. personal information).

There is also an internal need for the BBC to retain specific records for administrative, business and heritage purposes. Although the issuing office may no longer require these records, there may be a wider BBC need to retain them. It is the duty of the issuing office to see that this occurs. The BBC's retention schedule provides the framework for meeting these requirements.

All records must be included in the Records Retention Schedule. It is the responsibility of the issuing office to ensure their records have been identified. Document Archives should be informed of any records not covered by the Retention Schedule.

The Retention Schedule lists the following details about records:

- whether records are vital, important, useful, non-essential (*see Record Types*)
- location of the master copy
- the reasons for protection
- the agreed Retention period
- the storage media
- agreed action after retention period
- purpose of the records (legal, business, administrative)
- security marking of the record (confidential)

Records must not be destroyed before the retention periods expire. After the retention period has expired, non-essential records may be destroyed immediately; the request to destroy vital and important records must be submitted to Document Archives. Useful records may be destroyed immediately, unless the Retention Schedule advises they should be reviewed. Records with permanent value, whether for legal, business, or heritage reasons, must be transferred to the Written Archives Centre.

Any destruction of confidential records must be carried out in an appropriately secure manner.

If the status of records is altered, as the result of changes to legislation or business practices, Document Archives must be informed in order to update the retention schedule.

Secure storage

Records must be securely maintained to prevent unauthorised access, destruction, alteration or removal. It must be possible to prove that adequate protection is provided to ensure the integrity of the records for the purposes of internal and external audits. This is particularly important with records held in electronic environments where there may need to be additional proof that the records have not been altered. (*See Record Security*)

Records must be stored to a minimum standard that prevents them from being damaged or destroyed by environmental factors. (*See Storage Requirements*)

Access and retrieval

For records to have any value, it must be possible to identify, locate and retrieve them. In order to be able to locate records for retrieval they must comply with a minimum standard for metadata by which the unique record can be successfully identified (*See Metadata Requirements*).

It must be possible for any person with a legitimate right to access records to be able to retrieve them within an acceptable timeframe (*See Storage Requirements*). This is particularly important for any records that may need to be disclosed under the Freedom of Information Act.

Records held in paper format should be filed in chronological order and grouped logically within folders or files with meaningful titles. Folders and files should be labelled clearly, displaying the title, date range of the contents, and security marking if appropriate.

Meaningful Context

In order to understand the content of a record, it is also necessary to understand the context in which the record was created. For this reason it is necessary to capture relevant information at the point of creation. This information must meet the minimum standard for records metadata (*see Metadata Requirements*). The metadata must be maintained alongside the record regardless of any changes to the record-keeping system.

Where a number of records are connected (e.g. a chain of correspondence) it is important to ensure that links between them are maintained. This can be achieved through the use of folders and cross references.

It may be necessary to prove that records have been destroyed in accordance with established procedure. Contextual information should be retained, even if records have been destroyed.

Managing Electronic Records

Introduction

The requirements in the standard '*Managing Records in the BBC*' include both electronic records and paper records. This standard outlines further obligations that must be met for records held electronically.

Electronic Records Management Systems

There are a number of different Electronic Records Management products on the market. For a system to be implemented within the BBC must first meet the BBC's Electronic Records Management System functional specification and it must be passed by the relevant Controller or Head of Technology.

Record Integrity

The electronic environment provides a less stable format for holding records unless appropriate practices are employed. Improperly managed electronic records are more open to alteration, destruction or loss. For legal purposes it is important to be able to prove that documents have not altered or improperly destroyed. Records that are not held to an acceptable standard will lose much of their evidential status.

Security and Access

Security for electronic records should be managed through password control. This must not be limited to a single person; in the case of an emergency the records must be retrievable.

It is important to share all records that have a BBC business purpose with personnel who need regular access; therefore records must not be stored on personal areas (e.g. hard drives), but should be appropriately available.

Many current methods of storing documents electronically (e.g. shared drives) are not always suitable; the control of document security may not be adequate where access requirements are complex.

When leaving computers unattended it is important to secure them to prevent unauthorised access. (see *BBC Acceptable Use Policy* - http://guidelines.gateway.bbc.co.uk/dq/is/email_and_internet.shtml)

Protection

Sufficient back-ups must be in place to ensure that records are not lost due to hardware or software failure.

Migration

It must be possible to migrate records to another storage system for archival purposes or in cases where the electronic storage system becomes obsolete. All corresponding metadata must be exported alongside the records.

Where it is not practical to convert records from an obsolete format into a current format, or where the records have been compressed using software that is no longer in use, it will be necessary to retain the relevant software alongside the records to ensure continued access.

Integration with paper-systems

When paper records are being managed alongside electronic records, a stock control database, or file list, should be used to manage both concurrently. Alternatively, the paper records can be converted into an electronic format and managed within the existing electronic system.

Scanning

Documents must be scanned at resolutions that accurately reproduce the content; the electronic document must be no less useful than the original document.

Documents should be scanned at the following resolutions:

- Standard text documents should be scanned at a minimum resolution of 200 dots per inch (dpi).
- Drawings, maps and plans should be scanned at a minimum resolution of 300 dpi.
- Documents with faded text, or fine detail, should be scanned at a minimum resolution of 600 dpi.

When the original document can be read, but the scanned copy is not fully legible, it will be necessary to scan at a higher resolution than the recommended minimum.

If parts of the original document are illegible, it may be possible to adjust the scanner definition to restore legibility.

Once stored with an electronic system, scanned documents must be managed to the same standard as all other records.

Shared Folders and Email

Vital, important and useful records must not be stored within shared folders or email packages, as neither is suitable for long-term record management. Shared folders can be used to store non-essential records, or work-in-progress. Any records stored within shared folders that contain confidential or personal information must be marked as such and password-protected. Folders should also be identified as containing confidential material so that the IT service provider is aware. All records within shared folders must comply with the BBC's Retention Schedule.

Email should not be used to store records. Email accounts should be managed in accordance with the BBC's Acceptable Use Policy - (http://guidelines.gateway.bbc.co.uk/dq/is/email_and_internet.shtml#acceptableuse.) Where there is a need to keep emails, they should be transferred to shared drives, or proper records management systems.

Record Security

Introduction

Records must be maintained in an appropriately secure state. The levels of security must prevent unauthorised access to confidential records and also ensure that records cannot be altered.

Storage containers, including files, cabinets and electronic folders, containing confidential material must be marked to indicate this.

Government Classified material must be stored according to Government guidelines.

Physical Security

Records, particularly those containing information of a personal or commercially confidential nature, must be stored securely. Offices or cabinets containing such records must not be left unlocked and unattended.

Records that have been removed from their usual storage must be secured at their temporary location to an equal or better standard.

Electronic Record Keeping Systems

Electronic systems used for storing confidential records must comply with a minimum level of security (*see Managing Electronic Records*).

Access Control

Procedures should be put into place to ensure that confidential records are properly restricted. A list of personnel permitted access to the records should be compiled. The list should rely on roles rather than individuals for access rights; this reduces the need to update the list when changes in personnel occur. It is essential that the personnel accessing the records should be aware of the level of confidentiality required. Records must only be passed on to authorised staff.

Security Markings

Records must be marked according to their confidentiality. There are three levels of marking:

1. Non-sensitive – no marking required
2. Restricted to BBC Staff – mark as 'Confidential'
3. Restricted to a defined individual or group – mark as 'Restricted Access to (name of group/individual)'

If material is marked as Confidential or Restricted Access, a date must be given to indicate how long the material needs to remain confidential.

Any Government Classified material should be marked according to the Government requirements for markings and not the BBC requirements.

'CONFIDENTIAL' must appear on every page of a confidential document in either the header or the footer.

Any material that may bring undue media attention to the BBC if released must be marked as confidential.

Record tracking

The records holder should be aware of the whereabouts of all their vital and important records. Suitable tracking procedures should be put into effect. In the case of physical records, borrowers must inform the record holder of any further transfer. It is important that all electronic records management systems provide automated record tracking.

Integrity of Records

When records are complete they must not be altered. A new draft or version should be created if information in the original record is superseded, or incorrect, a new draft, or version, should be created. When migrating records from one storage medium to another (e.g. paper to electronic via scanning) it is important to retain the original content and layout.

Movement of Records Outside the BBC

If confidential information is moved over public networks, or taken outside the BBC on electronic storage devices, the data must be encrypted.

See BBC Information Security Policy

<http://guidelines.gateway.bbc.co.uk/dq/is/policies.shtml>

Metadata Requirements

Metadata provides a description, or profile, of a record. The description may contain data about the context, form or content of the record. The aims of metadata are to make content locatable, manageable and to provide context.

It must be possible to identify individual records either through a combination of metadata elements that only apply to a specific record, or through the assignment of unique codes.

A link should be maintained between a record and its metadata for as long as the record is held. If a record is destroyed, there may be a requirement to retain the metadata as proof that the destruction was carried out in compliance with the Retention Schedule.

Required Metadata Elements

Date of Creation. The creation date of a record should reflect the date of its authorship, or in the case of a contract it may be the date of sign-off. If a record is written over period of time, then the date it is completed should be used. In an electronic records management system the creation date should be captured automatically.

Date of Transaction. Where the transaction represented by the record differs from the date of creation (e.g. minutes of a meeting) the date of the transaction should be included as a separate metadata element.

Title. The title of a document should accurately reflect its content. Where possible the title should be unique. Naming should be consistent to assist with locating multiple records covering the same subject. Guidelines on naming of documents are available from Document Archives.

Retention Period. The record metadata should be linked to the Corporate Retention Schedule. The ultimate retention decision, along with any review periods, should be captured.

Author. The author of a record can be an individual, department or organisation. If a record has been received from outside of the corporation or from a different BBC department it is important to ensure that this information is captured.

Access control information. A list of personnel with access rights must be provided for restricted records. This should be linked to roles and responsibilities

rather than to individual employees. Security markings should be added to documents, where appropriate.

Links to other versions. When a new version of a record is created it is necessary to maintain a link to the other versions. This ensures the continuity of business processes. It may be necessary to provide evidence of changes and when they were made.

Location. Correct information about the location of a record is vital – without it the record is not retrievable and therefore worthless. It is necessary to record both the long-term storage location and any temporary location, if the record is on loan, for paper-based systems. The location of records is automatically captured within electronic record keeping systems.

Format. Within an electronic system, the format type of the record (e.g. Word document) will be automatically captured. In the case of a hybrid paper-electronic system it is important to register the records' storage media.

Storage Requirements

Introduction

There are a number of different options for storing records. The selection of the correct storage medium depends upon specific requirements. Consideration of possible legal issues should also be made before any changes to the storage media of records are made (e.g. microfilming contracts). When choosing storage options, the following should be considered:

- Access requirements
- Availability of storage space
- Cost
- Security
- Environmental issues

Digital Storage

Electronic records should be stored on a file server which undergoes regular back-ups. It is not recommended that records are stored on portable devices. CD-ROMs must never be used to hold Vital or Important records, even temporarily as these are prone to corruption

In the cases where CD-ROMs are appropriate, they should only be used to store records for a maximum of three years. It must not be possible to alter any information; therefore rewritable discs are not an appropriate storage medium. All CD-ROMs need to be stored in cool, dark, dry conditions.

Physical Storage Units

Storage units must have sufficient space to provide effective storage for records, whatever their size and shape. Shelving and cabinets must be strong enough to carry the potential load. It must be possible to secure the storage units if holding confidential records.

For health and safety reasons, the highest shelf should be reachable by a person of normal height, unless suitable alternative arrangements are made for safe access.

All efforts should be made to protect records from potential environmental damage, such as flooding, fire and vermin. Where a flood risk exists, the lowest shelf should be 85 -100 mm off the floor. Fire-proof safes should be used for storage of Vital records (*see Record Types*).

Physical storage must comply with the BBC's Health and Safety Policy.

Protection of Paper Records

Records in all formats deteriorate if not treated correctly. Simple measures can be taken to protect them from avoidable damage:

- Smoking, eating and drinking should be avoided near records and records storage areas.
- Paper records should not be stored in areas exposed to extremes of temperature, humidity and light.
- Some formats of paper, such as faxes printed from rolls, should be photocopied immediately as they are prone to rapid fading.
- Self-adhesive notes containing important comment which are stuck on documents should be copied separately and discarded. This avoids damage caused by deterioration in the glue and prevents accidental loss of the notes.
- When hole-punching paper documents care must be taken to avoid damage to the content.
- Appropriate files and folders should be used to store collated paper documents. Ring-binders and lever-arch files should not be used for Vital and Important records as they are more likely to cause damage.

Microfilm

Where there is a need to reduce physical storage space, microfilm may be an appropriate solution. When microfilm is used, it should be in accordance with the following British Standards:

- BS6498:2002 covering the preparation of microfilm that may be required as evidence
- BS5699-1:1979 covering using microfilm for archival records
- BS1153:1992 covering the process and storage of microfilm

Record Types

Records in the BBC are grouped, according to their importance to the corporation, into four categories. The categorisation affects the way the records should be managed, with more care being taken the higher the record's value.

Definitions

Vital. Vital records are those records that, if lost or destroyed, would have severe consequences to the BBC in terms of loss of money, reputation, or heritage. They are records that are either irreplaceable, or would be both costly and time consuming to recreate. They include those records that would be needed after an emergency or disaster to assist in the restoration of operability to the affected areas.

Important. Important records are those records that, in the event of their loss or destruction, can be reconstructed or replaced from other sources, although it may be costly and difficult to do so. They include those records that would be required after an emergency to support the vital records.

Useful. Useful records are those records that can be easily replaced. The time and cost of recreating these records would be minimal because the records, or the data they contain, are held elsewhere in the organisation and are easily accessible.

Non-Essential. Non-essential records are those records which have little or no value to an individual department and probably shouldn't have been retained. In the event of their loss or destruction there will be no need to recreate them.

Appendix A – Document circulation

Version Number	Created On	Author/Contributor	Circulation	Comments
01.02				