

BBSRC POLICY ON INFORMATION AND RECORDS MANAGEMENT

Document Control	
Version	1.0
Effective From Date	06 July 2009
Approved By	BBSRC Office Administration Group
Date of Approval	06 July 2009
Date of Review	06 July 2012
Retention Period	Indefinitely; 2 years after superseded
Owner	Communications and Information Management Group
Author	Melody Allsebrook

Contents

Policy Statement

Policy Scope

Policy Objectives

Policy Communication

Policy Responsibilities

Policy Principles

Definitions

Authenticity and Accountability

Appraisal

Naming Conventions

Metadata, Classification and Audit

Registration of Records

Duplication Management

Accuracy and Accessibility

Retention and Disposal

Security, Storage and Retrieval

Monitoring and Performance Measurement

Staff Training

Appendices –

- 1. Related Authoritative Bodies, Legislation, Standards and Codes of Practice**
- 2. Related BBSRC Policies and Strategies**
- 3. Document Control**

Annexes –

- A. Definitions/Glossary of Information and Records Management Terms**

Policy Statement

1. This policy is based on current Information and Records Management legislation, codes of practice, professional standards and regulations (listed at Annexes C and D). As a Non Departmental Public Body (NDPB) ¹, BBSRC is required to manage its information and records in compliance with this regulatory environment.
2. BBSRC recognises that having authentic, reliable and accountable records is a vital asset to the support of its daily business functions and operations.
3. BBSRC will deliver quality business information to support timely and effective decision making for planning, directing, controlling and reporting on its activities to form the corporate memory and enable delivery of BBSRC's strategic objectives. It will create the environment where:
 - a) information is properly created, managed and made accessible during its lifetime
 - b) information is only held whilst it holds value for BBSRC and is appropriately disposed of once it ceases to be an asset
 - c) information is shared, well defined, and publicised
 - d) the quality of the information is fit for purpose – it is accurate, up to date, relevant and complete
 - e) all staff understand and carry out their responsibilities towards the management of information

¹ NDPBs are independent of Government, but are accountable to Ministers who in turn are ultimately responsible to Parliament for the effectiveness of decisions made by NDPBs. BBSRC is accountable to the Department for Innovation, Universities and Skills.

Policy Scope

4. This policy applies to all information and records created or received in the course of day-to-day business, captured in a readable form, in any medium, and providing evidence of the events, functions, activities and transactions.
5. All BBSRC Office employees, whether permanent, temporary, contractors, consultants, or secondees will be hereafter referred to as 'staff'. All staff who have access to BBSRC information and records must comply with this policy.
6. This policy applies to both electronic and paper information and records created or received, unless otherwise stated.
7. All BBSRC information and records held within a paper file or on a corporate system, regardless of format, location or content, are the property of BBSRC.
8. This policy must be applied consistently across BBSRC Office by all staff; this includes BBSRC supported joint units (Joint Business Operations Services, Joint Superannuation Services and Research Councils Internal Audit Services).
9. Disciplinary action will be taken against staff failing to comply with this policy.

Policy Objectives

10. This policy aims to create an environment within BBSRC to achieve the following objectives:
- a) provision of a consistent and stable information and records management programme which is applied office wide
 - b) an office culture where all staff understand their responsibilities for the creation, use and management of information and records, and the value of that information is understood
 - c) office wide adherence to policies, guidelines and processes, supporting effective paper and electronic information and records management
 - d) identification of vital and critical records to enable business continuity in the event of a disaster
 - e) protection of information and records from inappropriate access, alteration, use, leakage or loss.
 - f) provision of evidence of actions and decisions
 - g) support for policy formulation and managerial decision making
 - h) protection of BBSRC's interests
 - i) protection of BBSRC's staff and stakeholders
 - j) accountability for BBSRC's past, present and future business operations
 - k) an awareness and understanding of BBSRC's history, research and processes
 - l) an open and transparent attitude to the dissemination of information into the public domain
 - m) the ability to communicate the results of BBSRC funded research as widely as possible
 - n) to contribute to the delivery, consistency and continuity of BBSRC operation services

Policy Communication and Related Information

11. A Glossary of Information and Records Management terms used in this policy is at Annex A.
12. BBSRC policies and strategies related to this policy are listed at Appendix 1.
13. BBSRC has an obligation to comply with the Information and Records Management legislation which is listed at Appendix 2.
14. BBSRC aims to comply with the Information and Records management Standards and Codes of Practice which are listed at Appendix 2.
15. This policy has been endorsed by BBSRC Senior Management and all staff will receive notification that mandatory adoption of the contents is required.
16. This policy will be reviewed regularly, as required or at least once every three years, in accordance with the Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act.²

² <http://www.dca.gov.uk/foi/reference/imp/imp/codemanrec.htm> Part 1: Records Management, Section 6 Policy, paragraph 6.3

Policy Responsibilities

Primary Responsibilities

Executive Responsibility	
Senior Information Risk Officer (SIRO)	Policy owner with accountability for its implementation. Responsible for maintenance of the information risk register, ensuring BBSRC's approach to information risk is effective and information threats and vulnerabilities are identified and followed up.
Head of Information Management	Responsible for execution of this policy's development, administration and application.
Head of Information Services	Responsible for implementing and applying Information Security policies, standards, guidelines and procedures; ensuring the security and accessibility of electronic information and records so that they are held in a robust format and remain readable for as long as they are required.
Information and Records Manager	<p>Responsible for development, administration, dissemination and application of this policy, and associated standards, guidelines and procedures.</p> <p>Responsible for administration, monitoring and maintenance of BBSRC electronic document and records management systems.</p> <p>Responsible for liaising with the off site storage provider and maintaining a good working relationship; providing a central point of contact between the provider and BBSRC Paper Records Administrators (PRAs).</p> <p>The Information and Records Manager will act as the 'Departmental Records Officer'³.</p>
Line Managers / Heads of Branch/Unit	<p>Responsible for ensuring their staff comply with this policy, attend training in the use of the electronic document and records management systems and attend information and records management awareness training.</p> <p>Responsible for ensuring their staff leavers do not leave any corporate information and records within inappropriate records storage areas (email system,</p>

³ The Public Records Act 1958 places responsibility for the management of public records on departments who must appoint a 'Departmental Records Officer'. Although BBSRC is not an official public body, it still has, as an NDPB, a duty to comply with the principles of the Act.
<http://www.nationalarchives.gov.uk/policy/act/system.htm>

BBSRC Information and Records Management Policy

	desktop, personal drive). Any information and records not transferred from these areas to the corporate electronic document and records management system(s) by the staff leaver will then become the responsibility of the Line Manager.
Paper Records Administrators	Responsible for the administration and management of all on site paper files held in their team or group custody, and any off site paper files owned by their team or group, in accordance with this policy and paper file management procedures.
Electronic Records Administrators	Responsible for the administration and management of their team/group electronic information and records within the corporate electronic document and records management system(s) and for providing a local point of contact for their team/group user queries. Issues for further investigation to be escalated with the Information and Records Manager.
All Staff	<p>All staff are responsible for the day to day management and protection of information and records they create or receive, from illegal or malicious activity, in accordance with this policy.</p> <p>All Staff have a duty to report any information leakage, compromise or loss and will be provided with a number of channels, including an independent and anonymous channel, through which they can report such events.</p> <p>All staff are responsible for ensuring they receive training on the corporate document and records management systems and attend appropriate information and records management training events.</p>

Supporting Responsibilities

Position	Responsibility
Chief Executive	Overall responsibility for BBSRC information and records.
Group Directors	Responsible for ensuring that this policy is supported and applied within their respective Groups.
Director CIMG	Responsible for supporting this policy's development, administration and application.

Office Administration Group	Responsible for the approval, endorsement and support of this policy and any subsequent amendments before its application.
Information and Policy Officer	Responsible for development, administration, dissemination and application of Freedom of Information policies, standards, guidelines and procedures.
Data Protection Officer	Responsible for development, administration, dissemination and application of Data Protection policies, standards, guidelines and procedures.

Policy Principles

Definitions

17. **Information and Records Management** is a policy driven method to ensure that information and records kept meet the business and operational needs as well as the legal and statutory requirements; it provides accountability to government, stakeholders and the academic community.

18. A **record** is an item in any format (documents, images, emails etc) containing the content, context and structure of all information required to give complete evidence of a business activity decision, action or transaction. The information contained within a record is a statement of fact that is fixed, cannot be altered and has a corporate retention period attached to it. A record must remain unaltered across time, no matter how many times it may be recalled for use or reference. A record may be superseded, but this then becomes a new document or record - the original record will remain unchanged. Records must be managed corporately and not by individuals or teams. Records can contain some or all of the following information which:

- a) provide evidence about policies, decisions, actions, transactions and activities (meeting minutes, confirmation letters, agreements etc), and interactions with stakeholders
- b) documents the rights and responsibilities of individuals and organisations
- c) contributes to BBSRC's history

19. During development of an electronic **record**, successive drafts may be kept (short term – standard duration of two years) as information, to provide evidence of the whole creation process and adequate proof of any substantial changes made during the development phase. Once published and declared as a record, it must be stored corporately within the electronic document and records management system.

20. A **document** is an evolving item of information; it is not fixed, it can be changed and edited, and is usually owned by an individual or a team. A document may be work in progress, may contain content, context or structure of information, but not

necessarily all three. Final versions of documents must be stored corporately within the electronic document and records management system.

21. **Paper Records management** is a policy driven method for the creation, receipt, management and control of paper files, from the point of their creation or receipt, through the duration of their set retention and any required review process to their destruction or transfer to a permanent archive.
22. **Electronic document and records management (EDRM)** is a policy driven method with the same principles as above. The EDRM system provides the platform for individuals to work collaboratively and manages the electronic information throughout its lifetime through to its disposal.

Authenticity and Accountability

23. An authentic, reliable and accountable record is one that can be proven to:
 - a) contain genuine content which can be trusted to be a full and accurate representation of the transaction or activity that took place
 - b) have been created or sent by the person said to have created or sent it (non-repudiation)
 - c) have been created or sent at the date and time claimed
 - d) have not been tampered with or altered in any way
 - e) be credible and authoritative so that evidence (as defined within the BBSRC Information Governance Forensics Policy) can be safely derived from it.

Naming Conventions

24. Information and records must be titled in accordance with the [BBSRC naming convention](#) guidance.

Metadata and Classification

25. The metadata associated with information stored within the EDRMS may include a combination of all or parts of the metadata from its original creation, as well as additional required metadata to support its storage and management within the EDRMS.
26. The corporate fileplan will be of a functional/activity based structure. This ensures that should the organisation undergo a restructure, the fileplan will never change as it will reflect the functions of BBSRC, although it may be added to.

Duplication Management

27. Duplicates of original records and documents should only be kept if there is a business or legal need to do so, otherwise duplicated copies of records and documents should be destroyed as soon as their immediate purpose has expired.

28. For both paper and electronic records and information, destruction applies to the original and **all** copies.

Accuracy and Accessibility

29. BBSRC information and records must be accessible and retrievable within a reasonable duration by those with a legitimate right of access, for as long as they are held by the BBSRC.
30. Appropriate controls and accounting measures will be in place to ensure security of the information and records maintained.
31. Appropriate measures must be taken to ensure information (paper and electronic) is handled securely should it need to be taken from the place of work. The measures should be in line with the sensitivity of the material.
32. Paper files are managed at group or team level by a group/team representative(s). Efficient and effective paper file tracking procedures must be followed to ensure that information and records can be located, accessed and retrieved with the minimum of delay. Storage conditions and handling processes must protect those records from unauthorised access, loss or destruction, theft or disaster.
33. Access to BBSRC information and records may be granted to eligible external users as required. In the event of an external user, such as an auditor, researcher or consultant requiring access, this may be granted following due consideration to ensure that any confidentiality obligations are maintained and continued in compliance with legislation. A confidentiality agreement must be completed and signed by the external individual(s) concerned and the relevant BBSRC business manager, with subsequent authorisation given by the Senior Information Risk Owner, the Information Security Officer and the Data Protection Officer.
34. Information and records must be identifiable, locatable and auditable. They must be securely stored, maintained and allocated appropriate confidentiality.
35. All electronic records must be managed at a corporate level within an EDRM system.
36. All information and records must be classified to maintain their confidentiality in accordance with a BBSRC Protective Marking Policy.

Retention and Disposal

37. Information and records must be kept for the agreed retention periods as stated in the [Retention Policy](#).
38. All personal data must be disposed of in a timely manner, and appropriate process, to comply with the Data Protection Act.
39. Paper and electronic inactive folders should be closed to new records at an appropriate time or size, whichever occurs soonest.

40. Destruction of electronic information and records within the EDRM system may only be carried out by the Information and Records Manager. A record must be kept of what has been destroyed.
41. Destruction Reports must be authorised by the relevant Business Manager and the Information and Records Manager and kept as a record of the date that the listed files were destroyed.
42. Destruction of paper and electronic information and records must be complete and unrestorable.
43. Paper files must be destroyed via shredding. If destruction takes place by a third party, evidence must be given to BBSRC.
44. Papers requiring destruction outside of the Office, ie at meeting venues, should be returned to the Office for shredding, unless the venue has appropriate destruction facilities, in which case this may be utilised.
45. Information and records found to be the subject of an investigation which are due for destruction must have their destruction temporarily halted until confirmation has been received that it/they is/are not subject to any regulatory investigation.
46. Disciplinary or legal action will be taken against staff who have deleted or attempted to delete information and records when they are part of a regulatory investigation.

Security, Storage and Retrieval

47. Information and records must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure should be properly controlled, with accounting logs to track all access, use and changes.
48. Appropriate measures must be taken to protect against the loss of information resulting from accidental or the malicious destruction of information or records.
49. Electronic information and records should be held in a robust format which remain readable for as long as they are required.
50. Information and records must be stored in an approved repository.
 - a) Electronic final document versions and records must be permanently stored within the appropriate repository (EDRMS) where possible; they should not be permanently stored in any other location, ie network drives, individual computer drives, removable storage devices or email system (see also paragraph 36.0).
 - b) Electronic information relating to awards and applications are held in the grants processing system and associated locations, and are subject to the relevant grants retention period.
 - c) Paper records must be stored within filing racks or cupboards on site, and tracked appropriately if moved, or within a bar coded archive box off site with

BBSRC Information and Records Management Policy

the approved storage provider. Contents and locations of all archive boxes must be recorded and known at all times.

51. Vital records must be stored securely and correctly for a period of time in accordance with the BBSRC Retention Policy. They should be quickly accessible, but not kept on the premises, in the event of a disaster to the building. Vital records must be kept in a form that can be read in the event of a disaster.

Monitoring and Performance Measurement

52. The application of records management procedures must be regularly monitored against agreed indicators, and action taken to improve standards as necessary.
53. BBSRC will endeavour to follow this policy within all relevant procedures used for business operational activities, and to regularly audit its records management practices for compliance. This will seek to:
 - a) Identify areas of operation not covered by the policy and to identify any procedures and/or guidance which need to adhere to the policy.
 - b) Set requirements by implementing new procedures, including obtaining feedback where the procedures do not match the desired activity.
 - c) Highlight where non conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

Staff Training

54. All staff must undertake annual information and records management awareness training to ensure they are aware of their information and record keeping responsibilities, and continue to comply with BBSRC policies, standards, guidelines and procedures.
55. All new staff, including temporary staff and consultants, must be made aware of the policy and their responsibilities through an Information and Records Management Induction process.

**APPENDIX 1
to BBSRC Information and Records Management Policy**

AUTHORITATIVE BODIES, LEGISLATION, STANDARDS AND CODES OF PRACTICE

INFORMATION AND RECORDS MANAGEMENT LEGISLATION AND STATUTORY REQUIREMENTS	
Data Protection Act 1998 ⁴	Reuse of Public Sector Information Regulations 2005 ⁵
Freedom of Information Act 2000 ⁶	Modernising Government White Paper 1999 ⁷
Public Records Act 1958 ⁸	HMG Security Policy Framework 2008 ⁹
Local Government (Access to Information) Act 1985 ¹⁰	HMG Information Assurance Standard 6 ¹¹
Access to Health Records Act 1990 ¹²	Lord Chancellor's Code of Practice of the Management of Records, Section 46 of the Freedom of Information Act ¹³

INFORMATION AND RECORDS MANAGEMENT BEST PRACTICE GUIDANCE AUTHORITIES
The National Archives (TNA) produces standards and guidance on all aspects of records management representing best practice for public records.
Joint Information Systems Committee (JISC) – advisory committee to the Research Councils providing expertise to support data and information management programmes.
British (and International) Standard for Records Management 15489-1:2001 and 2:2001
British (and International) Standard for Evidential Weight and Legal Admissibility of Information Stored Electronically. BIP 0008:2008

⁴ The Data Protection Act http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

⁵ Re-use of Public Sector Information Regulations <http://www.opsi.gov.uk/si/si2005/20051515.htm>

⁶ The Freedom of Information Act http://www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1

⁷ Modernising Government White Paper, Chapter Five: Information Age Government <http://www.archive.official-documents.co.uk/document/cm43/4310/4310-05.htm>

⁸ Public Records Act <http://www.nationalarchives.gov.uk/policy/act/>

⁹ Security Policy Framework <http://www.cabinetoffice.gov.uk/spf.aspx>

¹⁰ Local Government Act 1985 http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1985/cukpga_19850051_en_1

¹¹ HMG IA Standard 6 http://www.cabinetoffice.gov.uk/spf/sp4_isa.aspx

¹² Access to Health Records Act 1990 http://www.opsi.gov.uk/acts/acts1990/ukpga_19900023_en_1

¹³ Lord Chancellor's Code of Practice on the Management of Records <http://www.justice.gov.uk/guidance/docs/foi-section46-code-of-practice.pdf>

APPENDIX 2
to BBSRC Information and Records Management Policy

RELATED BBSRC POLICIES		
Document	Owner	Location
Information and Records Management Policy	Information Management	Office Policy Documents
Email Policy	Information Management	Office Policy Documents
Information Security Policy	Information Services	Office Policy Documents
Offline Working Policy	Information Management	Office Policy Documents
Employment Code: Appendix A2.2 - Use of Computer Facilities and Communications Systems	Information Services HRG	BBSRC Website
Employment Code: Appendix A12b:4i - Disciplinary Procedures	HRG	BBSRC Website
Freedom of Information Policy	Council Secretariat	BBSRC Website
Information Retention Policy	Information Management	Office Policy Documents
SharePoint New Starter Policy	Information Management	Office Policy Documents

LINKED BBSRC STRATEGIES, PROCEDURES AND GUIDES		
Document	Owner	Location
Information Management Strategy	Information Management	SharePoint Information Management Team Site
CE and Directors' Responsibilities for Corporate Records	Information Management	SharePoint Information Management Team Site
Information Storage and Naming Convention	Information Management	SharePoint Information Site
BBSRC Committee or Council Members Handbook	Council Secretariat	BBSRC Website

APPENDIX 3
to BBSRC Information and Records Management Policy

DOCUMENT CONTROL

VERSION CONTROL				
Version Number	Status	Creation/Revision Date	Author(s)	Summary of Changes
1.0	Record	06 July 2009	Melody Allsebrook	Policy Created

DISTRIBUTION FOR REVIEW			
Name	Title	Approved	Date
Eric Winiarski	Head of Information Management	Y	
Kathryn Turton	Head of Council Secretariat	Y	
Paul Chitson	Head of Information Services	Y	

TAGS	
Policy	Disposal
Record	Destroy
Information	Electronic
Retention	Paper
Management	Document

ANNEX A
to the Information and Records Management Policy:

GLOSSARY OF INFORMATION AND RECORDS MANAGEMENT TERMS

Access

Right, opportunity, means of finding, using or retrieving information.
[BS/ISO 15489]

Accountability

Principle that individuals, organisations, and the community are responsible for their actions and may be required to explain them to others. [BS/ISO 15489]

Appraisal

The process of evaluating information and records and making appropriate judgements before their creation, to establish their value to the business in terms of administrative, historic or operational requirements, enabling a decision on whether they should be retained, preserved or destroyed at the end of their useful life.

Archiving

The process of migrating or transferring inactive information and records from an active system to a repository for longer term storage and access.

Authentic

An authentic record is one that can be proven and trusted to be what it purports to be.

Business Activity

An umbrella term to describe all forms of BBSRC's organisational activity.

Classification

Systematic identification and arrangement of records into logically structured and categorised business functions and activities.

Corporate FilePlan

A hierarchical structure of classes starting with broad functional categories which are sub divided dependant on activities and subjects, until folders and documents are created at the lowest level.

Corporate Memory

A documented trail of and total body of data, information and knowledge providing evidence of corporate actions and decisions.

Critical Record

A vital record that must be protected from damage or destruction to ensure continuity of business functions and information flows.

Custody

Responsibility for the care of records or other material; usually based on paper possession of an object (file); the paper location of the object (file).

Data Protection

The law that governs the processing of personal information held on living, identifiable individuals. The Act requires that organisations are open about their use of information and that they follow eight certain principles for processing that information.

Destruction

Process of eliminating or deleting records that have no continuing value, beyond any possible reconstruction. [BS/ISO 15489]

Disposal (keeping, moving or removing records)

The range of processes associated with deciding whether to keep information and records for further review, destroy, or transfer records to a permanent archive to ensure their preservation.

See also **retention** and **appraisal**.

Document

An evolving item of information or object which is not fixed and can be changed and edited.

EDRM

Electronic Document and Records Management

Freedom of Information

The legal right, subject to certain exemptions, of the public to be informed of a public record's existence and the right to be supplied with it.

Information

A collection of data in any form, able to be manipulated and stored. Records are derived from information that constitutes evidence or memory of activity.

Legislation

Collections of rules imposed by authority. The act or process of law enactment by a legislative body (such as parliament).

Metadata

Data describing context, content and structure of records and their management through time. [BS/ISO 15489]

Metadata provides historical information and audit trails about information and records.

Migration

Process of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability. [BS/ISO 15489]

Preservation

Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time. [BS/ISO 15489]

Record series

A group of related records that are normally used and filed together or

otherwise linked and that allow consideration as a unit for use, review, retention or destruction purposes.

Record

Information created, received and maintained as evidence and/or information by an organisation or person, in pursuance of legal obligations or in the transaction of business. [BS/ISO 15489]

Records Management

Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, retention, retrieval, use and disposal of records. These include processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records. [Based on BS/ISO 15489]

Records System

Information system which captures, manages and provides access to records through time. [BS/ISO 15489]

Registration

Act of giving a record a unique identifier on its entry into a system. [BS/ISO 15489]

Registered File

An organised unit of documents dealing with the same subject, activity or transaction that is managed as a singular object and registered as above.

Regulatory Environment

Governmental Acts and Standards influencing and setting specific requirements on the creation and management of information and records.

Retention and Disposal Schedule

A management tool identifying and determining the retention periods and disposal decisions of information and records created by the organisation. Disposal is the range of processes that may follow a retention period, ie whether the information is retained for a further duration, destroyed or transferred to a place of permanent preservation.

Security

The handling, storage, viewing and disposal arrangements allocated to a record or document to protect the material to a level appropriate to its sensitivity.

Tracking

Creating, capturing and maintaining information about the movement and use of records. [BS/ISO 15489]

Transaction

A business agreement or exchange; an exchange of payment to gain an asset.

Transfer [custody]

Change of custody, ownership and/or responsibility for records. [ISO 15489]

Vital records

Information or records, in any form, that are essential to the continued operation and/or survival of the organisation after a disaster (business recovery). Vital records

BBSRC Information and Records Management Policy

are those necessary to recreate the organisation's legal and financial position and preserve its claims/rights and those of its stakeholders.