The Babraham Institute

BI-RES-006 Records Retention Policy

Document reference			
Policy number:	BI-RES-006		
Policy Owner:	Cass Flowers, Chief Information Officer		
Date:	01 July 2024		
Version:	2.0		
Status:	Active		
EIA number:	BI-RES-006-EIA		
Review period:	2 years		
Last reviewed:	01 July 2024	Next review:	August 2026

Version control			
Date	Version	Status	Summary of Changes
21 July 2021	1.0	Active	New in the 2021 Policy Review
01 July 2024	2.0	Active	Major changes requested in 2023 GDPR Governance RSM audit and new terms for corporate records retention

Document approval			
Define the approval authorities for the document			
Document version	Approved by	Position	Date
1.0	Babraham Executive Committee	N/A	21 July 2021
2.0	Babraham Executive Committee	N/A	05 September 2024

Distribution			
Date of issue		Version	
10/09/24		2.0	
This policy should be assigned to the following groups; Please tick one box for each group.			
Group Name	Mandatory	Group Name	Mandatory
All Users	☐	Heads of Department	☐
Trustees	☐	BCE Staff	☐
Researcher (Wet)	☐	Nursery	☐
Researcher (Dry)	☐	Visitors	☐
BSU Staff	☐	Credit Card Users	☐
BSU Users	☐	Ionising Radiation Users	☐

Notes: Optional for all Heads of Department and Trustees Only

Associated policies, procedures and guidance

This policy should be read in conjunction with:

Research records retention schedules, available on the GDPR pages of The Hub
Corporate records retention schedules, available on the GDPR pages of The Hub
BI-RES-001 Authorship Policy
BI-IM-002 Data Protection Policy
BI-IM-003 Information Classification & Security Policy
BI-KEC-001 Intellectual Property Policy
BI-RES-005 Research Integrity Policy
BI-COR-004 Business Continuity Plan
BI-RES-008 Research Data Management Policy
Guidelines for the use of Laboratory Notebooks, available on the H&S pages of The Hub
Code of Practice for Management of Electronic Scientific Data, available on the H&S pages of The Hub
A-Z Reference Guide to Retention Periods for H&S Records, available on the H&S pages of The Hub

Contents

1. Definitions

"Corporate records" Information in digital, computer-readable or paper-based format pertaining to the operational running of Institute business such as HR, finance, insurance, IT, governance, health and safety, etc.

"Data" Both paper records (e.g. printed documents, contracts, notebooks, letters and invoices) and electronic records (e.g. emails, electronic documents, audio and video recordings); the format is irrelevant when deciding whether or not a record should be retained. It applies to both personal data and non-personal data. In this policy we refer to this information and records collectively as "data".

"Research Data" Information in digital, computer-readable or paper-based format that:

- Is contained or presented in various ways, including notes, facts, figures, tables, images (still and moving), audio or visual recordings; and
- Which is collected, generated or obtained during the course of or as a result of undertaking research (which includes but is not limited to conducting field or laboratory experiments, conducting trials, surveys, interviews, focus groups or analysis of data); and
- Which is subsequently used by the researcher as a basis for making calculations or drawing conclusions to develop, support or revise theories, practices and findings.

"Research Records" All records relating to the conduct of a research project, including those that document the management of the research funds and the intellectual property. Research records typically include:

- All correspondence with granting agencies, institutions and collaborators.
- Funding records and correspondence relating to the grant financial records, purchasing records, scope of work, budgets, and service records.
- Approved protocols with all approved modifications for animal or human research, animal health records, surgical or treatment records, and breeding records.
- Records of research conduct, research quality and project management.

"Employee" Institute employees on Institute or Babraham Institute Enterprise Ltd (BIE) terms and conditions, Institute employees on BBSRC or other terms and conditions, and Research Fellows on Institute terms and conditions.

"Staff" Employees and Babraham Institute registered PhD students.

2. Commitment statement

2.1. At the Babraham Institute our mission is to be an international leader in research focusing on basic cell and molecular biology with an emphasis on healthy ageing through the human life course.

2.2. Research and operational excellence are essential to meeting our vision of being at the forefront of research that improves lives. The Institute Values set out our approach to how we operate across all Institute activities, both at an individual level and together as the Babraham Institute. The expectation of the Institute is that each staff member looks to represent and reflect the Institute Values within their own contributions and function, and to support and not hinder the expression of these Values in the work of others.

2.3. We recognise that the efficient management of records throughout their lifecycle is necessary to support its core functions, to comply with its legal and regulatory obligations, and to contribute to the effective overall management of the Institute.

2.4. For the avoidance of doubt, this policy does not form part of any Employee's terms and conditions of employment and may be amended by the Babraham Institute at any time.

3. Purpose

3.1. All researchers at the Institute create some type of data as part of the research workflow. These data represent the evidence that underpins academic endeavours and, in conjunction with publications, form an important aspect of the scholarly record. The corporate data and records of The Babraham Institute also is important to the Institute's function and employee management.

3.2. The Institute has legal and regulatory obligations to dispose of certain records after a set period. Effective records and data retention policies help underscore compliance with the General Data Protection Regulation (GDPR). Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. Furthermore, we do not need to retain all data indefinitely. Retaining data unnecessarily can expose us to risk, and is costly, both financially and with respect to the significant carbon footprint of data storage, which is at odds with our environmental commitments and net zero targets.

3.3. The Research Records Retention Schedules and Corporate Records Retention Schedules will, in time, identify vital and historically important records, which are suitable for transfer to longer term storage.

3.4. This Records Retention Policy serves the following purposes:

- Demonstrates that the Institute is committed to complying with all legal and regulatory requirements for data retention, including UK GDPR and DPA 2018.
- Explains Institute requirements to retain and dispose of both research and corporate records and provides guidance on appropriate data handling and disposal.
- Communicates the Institute's expectations about what data individuals may dispose of, along with when and how this may be done.
- Identifies who is responsible for records management, and the roles and responsibilities of all employees.

- Encourages disposal of unnecessary data before it becomes a liability or unnecessarily costly to retain.
- Helps protect data that may be relevant to a contemplated legal claim or regulatory or official investigation from being destroyed before the disclosure process.
- Safeguards proprietary data, which can help the Institute manage and reduce operational and reputational risks.

4. Scope

4.1. This policy applies to all those working with research records at the Institute, including:

- Institute employees on Institute or Babraham Institute Enterprise Ltd (BIE) terms and conditions
- Institute employees on BBSRC or other terms and conditions
- Research Fellows on Institute terms and conditions
- Research Fellows (honorary)
- Honorary Members of Faculty
- Babraham Institute registered PhD students
- Visiting students and visiting scientists (any relevant documents must be passed to the host before leaving the Institute)

4.2. This policy covers data that is stored:

- as hard copies in manual filing systems located on-site at the Institute (e.g. filing cabinets, offices, desks, drawers);
- as hard copies removed from Institute premises (e.g. notebooks, printed documents when working from home);
- on electronic systems / storage physically located at the Institute (e.g. Institute servers, desktop systems, enterprise storage facilities);
- on any electronic medium owned by the Institute, but removed from Institute premises (e.g. laptops, mobile devices, removable media);
- data stored by third-parties on our behalf (e.g. cloud storage providers, such as Microsoft SharePoint and OneDrive);
- on personal devices (BYoD) used to access Institute services and data in accordance with the Bring your own device policy (BI-BICS-002).

4.3. The Records Retention Schedules on the GDPR Hub pages (here) covers both paper and electronic records; the format is irrelevant when deciding whether or not a record should be retained. These schedules are derived from the Jisc Record Retention schedules.

4.4. This policy is compliant with the Institute's UKRI-BBSRC Terms and Condition of Grant. See 5.4 for consideration of other requirements.

5. Legislation & compliance framework

5.1. The management of records held by the Institute is regulated by the following legislation:

- Data Protection Act 2018[1] & General Data Protection Regulation (GDPR)[2].

[1] https://www.legislation.gov.uk/ukpga/2018/12/contents
[2] https://www.legislation.gov.uk/eur/2016/679/contents

- Freedom of Information Act 2000[3] (although the Institute is not directly required to answer Freedom of Information requests, the majority of our funders are. We therefore need to retain the required information).
- Limitation Act 1980[4].

5.2. The Data Protection and Freedom of Information Acts contain provisions relating to the destruction or alteration of information or records after a legal access request has been received. Such destruction or alteration will be considered a disciplinary offence. The Freedom of Information Act 2000 also creates a criminal offence in relation to these actions.

5.3. Other areas of the Institute's operations have specific retention requirements set out in separate legislation such as those relating to employment, health and safety, finance and pensions, and environmental information. We also require high quality records to be maintained for the purposes of audits and reviews by regulatory bodies.

5.4. Research data may also have specific requirements in relation to management, storage, retention and disposal set out under the terms of funding contracts, data sharing agreements, publishers, or by ethics committees that must be adhered to and which take precedence over this policy. It is the researcher's responsibility to understand such requirements as it relates to their research. Some funder requirements are included in the Research Records Retention Schedules (see here).

6. Responsibilities

6.1. The Institute has a corporate responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment. The Senior Information Risk Owner (SIRO) is accountable at an executive level for ensuring that appropriate provisions are in place. This role is held by the Institute's Chief Operating Officer.

6.2. The CIO is responsible for overseeing, supporting and monitoring our compliance with data protection laws which regulate personal data. The CIO works with the DPO to deliver specific advice on handling personal data. The strategy and planning of technical resources to meet the Institute's needs around Research Data Management is also a responsibility of the Chief Information Officer (CIO).

6.3. Babraham Executive Committee (BEC) are responsible for ensuring that this policy is regularly reviewed and is fit for purpose.

6.4. Heads of Department / Facility, Institute Strategic Programme (ISP) Leads and group leaders have overall responsibility for the management of records generated and held within their area.

6.5. There must be a clear allocation of responsibility within each department or team to assist with the management of records. All records should have an identified owner responsible for their management whilst in regular use, and for appropriate retention and disposal. This person or role is defined as the Information Asset Owner. There must be no ambiguity regarding responsibility for the maintenance and disposal of records.

[3] https://www.legislation.gov.uk/ukpga/2000/36/contents
[4] https://www.legislation.gov.uk/ukpga/1980/58

6.6. The Information Asset owner will normally be the group leader or head of department, although it is acceptable for them to delegate responsibility to another member of their group or department. Heads of Science Facilities may also manage data on behalf of the Information Asset Owner.

6.7. The Information Asset Owner will notify the CIO of any required changes to retention schedules (here), such as changes to retention period or the addition of new activities. They will also determine the following based on what is most appropriate for the records they manage:

- format of the record (electronic, paper etc.);
- storage location;
- retention trigger;
- retention period;
- reason for retention period (for instance, a relevant Act);
- action at the end of retention period (review for further retention, anonymise, destroy etc.);
- method of disposal.

6.8. Line managers are responsible for ensuring that their team is aware of this Records Retention Policy and comply with its requirements.

6.9. Individuals are responsible for ensuring that their work is documented appropriately, that the records which they create or receive are accurate and managed correctly, and are maintained and disposed of in accordance with the Institute's guidelines and any legislative, statutory and contractual requirements.

6.10. Line managers should ensure that when a member of their team leaves, responsibility for their records is transferred to another person; if any of the information is redundant, it should be deleted by either the departing individual or their line manager. It is vital that records management considerations are appropriately incorporated into project and planning processes and system design at the earliest possible stage of development. Where records contain personal data, there is a legislative requirement to do this in order to ensure that a “data protection by design and default” approach is followed. See the Data Protection Policy (BI-IM-002).

6.11. Please see Research Records Retention Schedules (here) and Corporate Records Retention Schedules (here) for details of the recommended retention periods. This information is based on the Jisc guide “retention schedules for information held in higher and further education institutions”.

7. Storage and disposal

7.1. All records must be stored in a safe, secure, and accessible manner. Hard copies must be stored in secure areas (e.g. locked offices, drawers, safes) that also offer suitable storage conditions and environmental controls to preserve the physical materials. Electronic copies must be stored in areas with restricted access that are secured using appropriate credentials.

7.2. The secure destruction of both hard copies and electronic data is the responsibility of the Information Asset Owner. Any personal data, or classified data (see BI-IM-003 Information classification and security policy) must be conducted securely, e.g. shredding hard copies. Unclassified data may be destroyed by recycling.

7.3. Record naming is the responsibility of the Information Asset Owner. Classified data should be named in accordance with naming and descriptors outlined in BI-IM-003 Information classification and security policy and research data should be identifiable in accordance with BI-RES-008 Research Data Management Policy.

7.4. Any data that is part of the activities listed in the retention schedules should be retained for the amount of time indicated in the Retention Period column. A record should not be retained beyond this period unless a valid business reason (or notice to preserve documents for contemplated litigation or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the CIO.

7.5. The retention schedules do not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of. If data is not listed in the retention schedules, it is possible it should be classed as disposable information. However, if you believe that there is an omission, or if you are unsure, contact the CIO.

8. Special circumstances

8.1. All individuals should note the following general exception to any disposal: If you believe, or are informed, that certain records are relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the SIRO determines those records are no longer needed. Preserving documents includes suspending any requirements in the retention schedules and preserving the integrity of the electronic files or other format in which the records are kept.

8.2. In addition, you may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as the replacement of an IT systems or group departure.

9. Breach of policy

9.1. The Institute's Disciplinary Policy (BI-HR-005) may be invoked if you breach the Records retention policy.

10. Further information

7.1. For more information and guidance on GDPR, see the ICO website[5], the Jisc GDPR page[6] and Records Retention Management | Jisc[7]

7.2. This policy will be reviewed regularly to incorporate any changes, legislative or otherwise. The next review date is specified on the cover sheet.

7.3. Associated policies, procedures and guidance are listed on the cover sheet. The Policy Owner named on the cover sheet can be contacted with any queries.

[5] https://ico.org.uk/
[6] https://www.jisc.ac.uk/gdpr
[7] https://www.jisc.ac.uk/guides/records-retention-management

7.4. This policy may be varied, withdrawn or replaced at any time by the Institute at its absolute discretion.