The Babraham Institute

BI-IM-002 DATA PROTECTION POLICY

Document reference			
Policy number:	BI-IM-002		
Policy Owner:	Cass Flowers, Chief Information Officer		
Date:	01 December 2020		
Version:	1.2		
Status:	Active		
EIA number:	BI-IM-002-EIA		
Review period:	3 years		
Last reviewed:	10 February 2023	Next review:	August 2025

Version control			
Date	Version	Status	Summary of Changes
01 December 2020	1.0	Archived	Updated in the 2020 Policy Review
13 October 2021	1.1	Active	Updates to clarify 6.5; removal of civil proceedings information from Further information (all policies)
10 February 2023	1.2	Active	Updates to reference DPIA, LIA, and other procedures.

Document approval			
Define the approval authorities for the document			
Document version	Approved by	Position	Date
1.0	Policy Review Working Group	N/A	01 December 2020
1.1	Karen Vincent	Head of Governance	13 October 2021
1.2	Stephen Barrett	Project Officer	10 February 2023

Distribution		
Name or Group	Date of issue	Version
All staff and associates	02 February 2021	1.0
All staff and associates	13 October 2021	1.1
All staff and associates	10 February 2023	1.2

Associated policies, procedures and guidance
This policy should be read in conjunction with:
BI-IM-002-SOP-001 Data Breach Procedure BI-IM-002-SOP-002 Data Subject Rights Request Procedure

BI-BICS-001 IT Security and Usage Policy
BI-BICS-002 Bring Your Own Device Policy
GDPR and Data Protection Pages on The Hub
BI-RES-006 Research Records Retention Policy
Data Protection Impact Assessment (DPIA) Template
Legitimate Interests Assessment (LIA) Template

Contents

1. Definitions

"Data Controller"	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
"Data Protection Officer"	The senior manager who is responsible for ensuring that an organisation follows its data protection policy and complies with the Data Protection Laws.
"Data Protection Laws"	Any applicable law relating to the processing, privacy and use of Personal Data, including the Data Protection Act 2018 and the GDPR and any laws that replace, extend, re-enact, consolidate or amend any of the foregoing.
"Data Subject / Service User"	The individual whose personal information is being held or processed by the Babraham Institute (e.g., a service user or a supporter).
"Explicit Consent"	A freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about themselves.
"Notification"	Notifying the Information Commissioners Office (ICO) about the data processing activities of the Institute and subsidiary companies. Note: not-for-profit organisations are exempt from notification but the Institute has registered with the ICO as we are not exempt from reporting data breaches.
"Information Commissioner"	The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018 and the GDPR.
"Processing"	Collecting, amending, handling, storing or disclosing personal information.
"Processor"	Means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.
"Personal Information / Personal Data"	Information about living individuals (data subject) that enables them to be identified, e.g., names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual collaborators of the Babraham Group.
"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.
"Associates"	Research Fellows (honorary), Honorary Members of Faculty, visiting students, visiting researchers and workers (including consultants and secondees), workers provided by a third party / contractors, and Trustees.
"Individuals"	Staff, associates, visitors and members of the public.

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 are committed to protecting the rights and privacy of individuals. We need to collect and use certain types of data in order to carry out our work. This personal information will be collected and dealt with in accordance with data protection laws. We are committed to being transparent regarding the collection and use of personal data.

2.4. The Institute is committed to meeting the GDPR requirement to assess data privacy at the initial design stages of a project as well as throughout the lifecycle of the relevant personal data processing.

3. Purpose

3.1. The purpose of this document is to set out the Institute's commitment and procedures for protecting personal data. The Board of Trustees regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. Failure, on the part of any member of staff or associate, to comply with this policy, will be subject to disciplinary procedures.

3.2. The General Data Protection Regulations ("GDPR") in force from 25 May 2018 replaced The Data Protection Act 1998 and governs the use of Personal Data. The GDPR principles have been incorporated into the Data Protection Act 2018, which achieved Royal Assent and became UK law on the 23 May 2018. Following the UK's exit from the EU, this became "UK GDPR" on 01 January 2021.

3.3. Personal data may be held electronically or as a hard copy. It may be stored on computer systems, mobile devices, storage media, or in a manual (i.e., paper-based) file. It includes,

but is not limited to, email; meeting minutes; interview notes; video recordings; and photographs.

3.4. The Institute will remain the data controller for the personal information held. Institute staff and associates are personally responsible for processing and using personal information in accordance with the Data Protection Act 2018/EU GDPR/UK GDPR referred collectively within this policy as "GDPR".

3.5. Staff and associates who have access to personal information are required to read and comply with this policy.

4. Scope

4.1. This policy applies to:

- 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
- Visiting researchers and workers, including consultants and secondees
- Workers provided by a third party / contractors
- Trustees

4.2. Members of the public, including service users, supporters, interviewees or ex-employees may also raise Subject Access Requests or complaints under this policy (See section 6.5).

4.3. Aspects of this policy are available on the Institute website. Copies will be made available upon request.

5. The General Data Protection Regulations

5.1. Under the GDPR, the data protection principles set out the main responsibilities for organisations.

5.2. Article 5 of the GDPR requires that personal data shall be:

- Processed fairly and lawfully and, in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.3. Article 5(2) requires that:

- The Controller shall be responsible for, and be able to demonstrate, compliance with the principles.

6. Applying the General Data Protection Regulations within the Institute

6.1. Lawful basis for processing data

6.1.1. The lawful bases for processing are set out in Article 6 of the GDPR, they are:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

d) **Vital interests:** the processing is necessary to protect someone's life.

e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

6.1.2. The lawful bases on which the Institute most commonly processes personal data is:

- That it is necessary to fulfill our contract with employees and suppliers, e.g., processing payroll and supplier payments;
- That it is necessary to comply with our legal obligations;
- That it is in our legitimate business interest, e.g., details of our research, publications and collaborators;
- That an individual has given consent to processing, and may later withdraw this consent to stop processing;

6.1.3. In accordance with Article 30, the Institute maintains a central Record of Processing Activity (RoPA) which documents personal data processing activities under our responsibility.

6.1.4. The Institute may pass personal information to:

- Regulatory bodies.
- Institute internal and external auditors, and the Government Internal Audit Agency.
- Any processor (individual / organisation) that we use to provide goods or services, e.g., Babraham Research Campus Ltd (BRC) who provide security services to the Institute.

6.2. Individuals' rights

6.2.1. Individuals have a number of rights in relation to their personal data:

- The right to be informed;
- The right of access (See section 6.5);
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- The right not to be subject to automated decision-making, including profiling.

6.2.2. Individuals have a right to have personal data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

6.2.3. The Data Subject Rights Requests Procedure (BI-IM-002-SOP-002) provides a framework for all staff to refer to when handling a data subject rights request.

6.3. Personal data breaches

6.3.1. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

6.3.2. The Institute will treat any personal data breach very seriously and will fully investigate any such breach. Full records will be kept within the Institute's Data Breach Register and maintained by the CIO.

6.3.3. The GDPR imposes a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. This should be within 72 hours of becoming aware of

the breach, where feasible. The Information Commissioner's Office (ICO) is the supervisory authority for the United Kingdom.

6.3.4. Individuals will be informed of any personal data breach that could adversely affect them.

6.3.5. All staff and associates must report the loss of personal data immediately when the loss is discovered. This must be reported immediately to the Chief Information Officer and/or dpo@babraham.ac.uk.

6.3.6. The Data Breach Procedure (BI-IM-002-SOP-001) provides a framework for all staff to refer to should a data breach occur.

6.4. Responsibilities

6.4.1. The Institute is the data controller under the GDPR, and is legally responsible for complying with GDPR, which means that it determines what purposes personal information held will be used for.

6.4.2. The Babraham Executive Committee (BEC) will consider all GDPR requirements and ensure that it is properly implemented. It will do this through appropriate management and strict application of criteria and controls.

6.4.3. Staff and associates are responsible for helping the Institute keep their personal data up to date. Staff and associates should inform the Institute if the personal data they have provided to the Institute changes, e.g., if they move house or change bank details.

6.4.4. Staff and associates may have access to the personal data of other individuals, including other members of staff, visitors, collaborators and customers, in the course of their work. Where this is the case, both the Institute and the member of staff or associate are responsible for ensuring compliance with data protection obligations.

6.4.5. It is therefore important that all staff and associates consider any information, which is not otherwise in the public domain, that can be used to identify an individual and is therefore personal data, and observe the guidance in section 6.8 (Institute GDPR Operational Guidance).

6.5. Data subject access requests (DSAR/SAR) & complaints

6.5.1. The Data Subject Rights Requests Procedure (BI-IM-002-SOP-002) provides a framework for all staff to refer to when handling a subject access request or complaint.

6.5.2. Individuals have the right to make a subject access request under the GDPR for access to personal information that the Institute processes about them. If an individual makes a subject access request, the Institute will take appropriate action. This may include providing the individual with a copy of their personal data.

6.5.3. If a request is valid, the Institute will action the request without undue delay and within one month. If a request is refused, the Institute will tell the individual why. It will also inform the individual that they have the right to complain to the supervisory authority. The Institute will not charge for any reasonable access request.

6.5.4. Subject access requests or data complaints received by any member of staff or associate must be reported immediately to the Chief Information Officer and/or dpo@babraham.ac.uk.

6.5.5. All data subject access requests should be made directly to the Chief Information Officer via the DPO email mailbox dpo@babraham.ac.uk.

6.5.6. Data subject requests will be recorded within the Institute's Data Subject Rights Register, by the CIO, and updated with actions taken.

6.6. Data protection by design & impact assessments

6.6.1. The GDPR makes privacy by design an express legal requirement, under the term "Data protection by design and by default" (Art. 25 GDPR). It also makes Data Protection Impact Assessments (DPIA) mandatory for operations that present a high risk to the rights of an individual (Art. 35 GDPR).

6.6.2. The Institute will undertake a DPIA in high-risk circumstances, such as the examples listed below. A full list of screening questions are available within the Institute's DPIA template:

- A new system involving personal data is being implemented.
- Personal data will be disclosed to organisations or people who have not previously had access to it, e.g. using a new cloud-based service.
- There is processing on a large scale of the special categories of personal data.

6.6.3. Where an operation doesn't meet the circumstances outlined in the DPIA screening questions and the processing will be done under the lawful base of legitimate interests, the Institute will perform a Legitimate Interests Assessment (LIA).

6.6.4. DPIA and LIA templates are available on the GDPR and Data Protection pages on The Hub, along with guidance to support completion. Impact assessments are also integrated into the Institute's Project Governance Framework to ensure any risk is considered at project initiation, if it may involve processing personal data.

6.6.5. Special category personal data is particularly sensitive under GDPR, including but not limited to, physical or mental health, ethnicity, religion, biometric data (e.g. fingerprints), and trade union membership.

6.6.6. Records about submitted DPIAs/LIA will be recorded within the Institute's DPIA and LIA Register, and regularly updated.

6.7. Procedures for handling data & data security

6.7.1. Companies have a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- Unauthorised or unlawful processing of personal data;
- Unauthorised disclosure of personal data;
- Accidental loss of personal data.

6.7.2. All staff and associates must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used.

6.7.3. Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary, opinion or religious beliefs etc. would be classed as personal data, and falls within the scope of the data protection laws.

6.8. Institute operational guidance

6.8.1. Email

6.8.1.1. All staff and associates should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained, it should be stored in a secure location rather than an email mailbox. The original email should then be deleted from the mailbox and any deleted items area, either immediately or when it has ceased to be of use.

6.8.1.2. Remember, emails that contain personal information which is no longer required for operational use, should be deleted from your personal mailbox and any deleted items area.

6.8.2. Phone calls

6.8.2.1. Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- If you receive a phone call asking for personal information to be checked or confirmed, be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access. If they are genuine data subject access requests they should be passed to the CIO to handle.
- Personal information should not be disclosed over the telephone unless you have no doubts as the caller's identity and their right to the information. Acceptable cases whereby information may be provided include:
    - The HR or Payroll team speaking to an employee about their own data; and,
    - Satisfying statutory obligations.

  If you have any doubts, ask the caller to put their enquiry in writing.

6.8.3. Mobile devices and data security

6.8.3.1. All Institute data should be stored on Institute storage services. Store as little personal data as possible on your computer or mobile device; only keep those files that are essential.

6.8.3.2. All computers and mobile devices that hold personal information should be encrypted.

6.8.3.3. Ensure your computer is locked (password protected) when left unattended, even for short periods of time.

6.8.3.4. When travelling in a car, make sure your mobile devices are stored out of sight, preferably in the boot. If you must leave your device in an unattended vehicle at any time, put it in the

boot and ensure all doors are locked and any alarm set. Never leave devices in your vehicle overnight.

6.8.3.5. Do not leave devices unattended in restaurants or bars, or any other venue.

6.8.3.6. When travelling on public transport, keep your device with you at all times, do not leave it in luggage racks or even on the floor alongside you.

6.8.4. Passwords

6.8.4.1. All passwords used to access Institute services or data must conform to the password and security terms outlined in the IT Security and Usage Policy (BI-BICS-001).

6.8.4.2. Any personal devices used for work purposes must also be secured from unauthorised access, as outlined in the Bring Your Own Device Policy (BI-BICS-002).

6.8.5. Data storage

6.8.5.1. Personal information and records relating to service users will be stored securely and will only be accessible to authorised staff and associates.

6.8.5.2. Personal information will be stored only for as long as necessary and will be disposed of appropriately when no longer necessary.

6.8.5.3. The Institute shall ensure any personal data and company data is unrecoverable from any computer system previously used within the Institute that has been passed on / sold to a third party.

6.8.5.4. This policy will be updated as necessary to reflect best practice in personal data management, security and control and to ensure compliance with any changes or amendments made to any data protection laws.

6.9. Freedom of Information Requests

6.9.1. The Freedom of Information Act 2000 was introduced to increase accountability of public bodies by enabling members of the public to request disclosure of information such as decision-making processes and internal practises. The Act does not apply to the Institute, but we are still required to respond to requests for information where information shared with a public body, e.g., as part of a tender or procurement contract, is subject to a Freedom of Information request. The information will be published under the public body's publication scheme and in accordance with data protection laws.

7. Disclosure

7.1. We may need to share personal data with other agencies such as the local authority, funding bodies, and other voluntary agencies.

7.2. The data subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where data protection law allows the Institute to disclose personal data, including special category data, without the data subject's consent. These are when:

- Carrying out a legal duty or as authorised by the Secretary of State protecting vital interests of a data subject or other person.
- The data subject has already made the information public.
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
- Monitoring for equal opportunities purposes, e.g., race, disability or religion.
- Providing a confidential service where the data subject's consent cannot be obtained or where it is reasonable to proceed without consent, e.g. where we would wish to avoid forcing distressed or ill data subjects to provide consent signatures.

7.3. Any transfers of data made outside of Sections 7.1 or 7.2 must be recorded and provided to the CIO. This must include the date the information was provided, to whom, for what purpose and the categories of data.

7.4. We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

7.5. We intend to ensure that personal information is treated lawfully and correctly.

8. Risk management

8.1. The consequences of breaching data protection laws and best practice can cause harm or distress to data subjects if their information is released inappropriately, or they could be denied a service to which they are entitled.

8.2. Staff and associates should be aware that under the GDPR, they can be held personally liable if they use personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the Institute and the rights and freedoms of individuals are not damaged through inappropriate or unauthorised access and sharing of personal data.

9. Destroying personal data

9.1. Personal data should only be kept for as long as it is necessary and appropriately destroyed when no longer necessary.

9.2. We will review personal data processing activities regularly and will ensure that personal information is confidentially destroyed at the end of the relevant retention period.

10. Further information

10.1. For further information see the Information Commissioner's website: http://www.ico.org.uk/

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

10.3. 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.

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