The Babraham Institute

BI-IM-003 INFORMATION CLASSIFICATION & SECURITY POLICY

Document reference			
Policy number:	BI-IM-003		
Policy Owner:	Cass Flowers, Chief Information Officer		
Date:	16 August 2023		
Version:	1.2		
Status:	Active		
EIA number:	BI-IM-003-EIA		
Review period:	3 years		
Last reviewed:	August 2023	Next review:	August 2026

Version control			
Date	Version	Status	Summary of Changes
01 December 2020	1.0	Active	Updated in the 2020 Policy Review
20 July 2022	1.1	Active	Minor formatting amendments only.
16 August 2023	1.2	Active	Section 8 added on use of AI Chatbots

Document approval			
Define the approval authorities for the document			
Document version	Document approved by	Position	Date
1.0	Policy Review Working Group	N/A	01 December 2020
1.1	Stephen Barrett	Project Officer	21 September 2022
1.2	Stephen Barrett	Project Officer	14 September 2023

Distribution			
Date of issue		Version	
14/09/2023		1.2	
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 Trustees			

Associated policies, procedures and guidance
This policy should be read in conjunction with:
BI-IM-002 Data Protection Policy BI-BICS-001 IT Security & Usage Policy

Contents

1. Definitions

"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.

"Individuals" Staff, Research Fellows (honorary), Honorary Members of Faculty, visiting students, visiting researchers and workers (including consultants and secondees), workers provided by a third party / contractors, visitors, and Trustees.

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 appropriately protecting our information assets, whilst allowing for effective exploitation of information.

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. This policy is drafted in line with HMG Cabinet Office direction for the implementation of an organisation-wide security classification policy and is compatible with UKRI-BBSRC confidentiality requirements. This policy describes the expectation of Institute individuals to appropriately protect information assets, allowing for the effective exploitation of information and to ensure the Institute meets the requirements of all relevant legislation and contractual obligations.

3.2. The purpose of this policy is to provide guidance for the management of information collected, stored, processed, generated, or shared by the Institute.

3.3. This policy should be used in accordance with all other Institute policies, including the Data Protection Policy (BI-IM-002) and IT Security & Usage Policy (BI-BICS-001).

4. Scope

4.1. This policy applies to all information owned, controlled or in possession of the Institute, whether in electronic or hardcopy format.

4.2. All Institute individuals are expected to take responsibility for the information they manage. Institute individuals have a duty to respect the confidentiality and integrity of any Institute information and data assets that they hold and / or access and are personally accountable for safeguarding assets in line with this policy.

4.3. 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
- Visitors
- Trustees

5. Principles

5.1. Principle one

5.1.1. **ALL** information that the Institute collects, stores, processes, generates, or shares to conduct research or deliver services has intrinsic value and requires an appropriate degree of protection.

5.1.2. Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss, or misuse) and the need to defend against a broad profile of applicable threats. There are three levels of classification:

CONFIDENTIAL	CONFIDENTIAL-SENSITIVE	SECRET
The majority of information that is created or processed by the Institute shall be classified as CONFIDENTIAL. This includes routine business operations, services, research results and / or unpublished information, some of which could have damaging consequences if lost, stolen, or disclosed inappropriately.	A subset of CONFIDENTIAL information that could have more severe consequences if lost, stolen, or disclosed inappropriately. This information shall be managed in line with CONFIDENTIAL information but with the additional measures to reinforce a 'need to know' basis. Information falling into this tier includes personnel information and personal data.	Applies to highly sensitive information requiring heightened security measure. This covers information that could have severe detrimental legal consequences or reputational damage if lost, stolen, or disclosed inappropriately. Institute individuals are less likely to receive or handle information considered SECRET.

5.1.3. Each classification provides for a baseline set of personnel, physical and information security controls that offer an appropriate level of protection. As a minimum, all Institute information must be handled with care to comply with legal and regulatory obligations and reduce the risk

of loss or inappropriate access. There is no requirement to mark information that does not fall into the above three categories.

5.2. Principle two

5.2.1. **EVERYONE** who works with the Institute (including all Institute individuals and service providers) has a duty of confidentiality and a responsibility to safeguard any Institute information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate guidance.

5.2.2. Accidental or deliberate compromise, loss or misuse of Institute information may lead to damage and can constitute a criminal offence. Individuals are personally responsible for protecting any Institute information or other assets in their care and must be provided with guidance about security requirements and how legislation relates to their role, including the potential sanctions (criminal or disciplinary) that may result from inappropriate behaviours.

5.2.3. See 'Use of AI Chatbot Technology' (Section 8) for guidance on complying with this policy if using AI Chatbots for work purposes.

5.3. Principle three

5.3.1. Access to sensitive information must **ONLY** be granted based on a genuine "need to know" and an appropriate personnel security control.

5.3.2. Information needs to be entrusted and available to the right people at the right time. The failure to share and exploit information can impede effective Institute business and strategy, and can have severe consequences (e.g., loss or disclosure of personal data or employee files). The principles of openness, transparency, Open Data and information reuse require Institute individuals to consider the proactive publishing of information and data sets. However, this must always be a reasoned judgement, taking data protection legislation (see the Institute Data Protection Policy [BI-IM-002]), confidentiality requirements and obligations into account.

5.3.3. The compromise, loss or misuse of sensitive information may have a significant impact on an individual, an organisation, or on Institute business more generally. Access to sensitive information must be no wider than necessary for the efficient conduct of the Institute's business and limited to those with a business need and the appropriate personnel security control. This "need to know" principle applies wherever sensitive information is collected, stored, processed, or shared within the Institute and when dealing with external public and private sector organisations, and international partners.

5.3.4. The more sensitive the material, the more important it is to fully understand (and ensure compliance with) the relevant security requirements. In extremis, there may be a need to share sensitive material to those without the necessary personnel security control, e.g., when immediate action is required to protect life or to stop a serious crime. In such circumstances a common-sense approach should be adopted – if time permits, alternatives should be considered, and steps taken to protect the source of information. If there is any doubt about providing access to sensitive assets, individuals should consult their managers or the Chief Information Officer (CIO) before doing so and, when time permits, record the reasons for their actions.

5.4. Principle four

5.4.1. Assets received from or exchanged with external partners **MUST** be protected in accordance with any relevant legislative or regulatory requirements, including any agreements and obligations.

5.4.2. The policy applies equally to assets entrusted to the Institute by others, such as collaborators, commercial clients, and private individuals.

5.4.3. Where specific reciprocal agreements / arrangements are in place with external or international organisations, equivalent protections and markings must be recognised and any information received must be handled with AT LEAST the same degree of protection as if it were Institute or UK information of equivalent classification.

5.4.4. Where no relevant agreements / arrangements are in place, information or other assets received from an external or international organisation or a UK organisation must at a minimum be protected to an equivalent standard as that afforded to Institute information assets, although higher classifications may be appropriate.

6. Descriptors

6.1. Security classifications are the principle means of indicating the sensitivity of a particular asset and the requirements for its protection. Special handling instructions are additional markings that can be used in conjunction with a classification marking to indicate the nature or source of its content, limit access to designated groups, and / or to signify the need for enhanced handling measures.

6.2. Special handling instructions should be used sparingly and only where the sensitivity justifies strict restrictions on information sharing. Individuals must be given guidance on how to mark and work with assets bearing special handling instructions.

6.3. Individuals may apply a DESCRIPTOR to identify certain categories of sensitive information and indicate the need for common sense precautions to limit access. Where descriptors are permitted, they must be supported by local policies and business processes. Descriptors should be used in conjunction with a security classification and applied in the format: 'CONFIDENTIAL -SENSITIVE [DESCRIPTOR]'

6.4. The Institute maintains the following list of core descriptors to ensure a consistent approach is adopted across all departments:

- **'COMMERCIAL'**: Commercial or market-sensitive information, including that subject to statutory, contractual, or regulatory obligations, which may be damaging to the Institute or to a commercial partner if improperly accessed.
- **'PERSONAL'**: Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, or the personal records / personal data of people.

6.5. When working with information assets, the following points need to be considered:

- Applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls.

- Applying too low a marking may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise.
- When working with documents, classifications must be in CAPITALS at the top and bottom of each page. More sensitive information should be separated into appendices, so the main body can be distributed widely with fewer restrictions.
- Sensitive material published on intranet sites, e.g., The Hub, must also be clearly marked.
- It is good practice to reference the classification in the subject line and / or text of email communications. Where practicable, systems should compel users to select a classification before sending, e.g., via a drop-down menu.
- Only originators can classify an asset or change its classification, though holders of copies may challenge it with a reasoned argument. Every effort should be made to consult the originating organisation before a sensitive asset is considered for disclosure.
- A file, or group of sensitive documents or assets, must carry the highest marking contained within it. For example, a paper file or an e-mail string containing CONFIDENTIAL and SECRET material must be covered by the higher marking (i.e., SECRET).
- E-mails are often conversational documents, added to by several people in response to a query or question. Individual recipients must assess the entire contents of an e-mail "trail" before they add to it and forward it on.
- In certain circumstances there may be a good reason to share selected information from a sensitive report more widely. Originators should consider whether it is possible to develop a sanitised digest or pre-agreed form of words at a lower classification in anticipation of such a requirement.
- Where practicable, time-expiry limits should be considered so that protective controls do not apply for longer than necessary, this is particularly the case for embargoed material intended for general release and only sensitive until it is published, e.g., publication of results or data.

7. Information handling instructions

7.1. See Appendix 1 for detailed information handling instructions.

8. The use of AI Chatbot technology

8.1. As technology continues to advance, use cases for Artificial Intelligence (AI) in the workplace continue to grow and have the power and potential to improve efficiency and productivity.

8.2. All information you enter into an AI Chatbot may be stored and used by the creator. **You must always be very careful when using AI Chatbots and never input any classified or personal data.**

8.3. The main output of most AI chatbots is a wrap-up of content from the Internet. Please remember that not everything on the Internet is true or a reliable source of information. Always verify the information you receive prior to using AI generated outputs for work purposes.

9. Further information

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

9.2. 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.

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

Appendix 1 – Information handling instructions

	CONFIDENTIAL	CONFIDENTIAL-SENSITIVE (to be used in addition to CONFIDENTIAL)
Legal and statutory requirements must be followed regardless of classification, in particular data protection legislation (the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018).		
General	• Be stored and managed in line with Institute approved systems. • Used in accordance with clear desk / screen policy. • Not to be accessed, read or discussed in areas where you can be overlooked or overheard. • Not to be left on desks or in areas where others may be access it.	• Not be left unattended and should be locked away when not in use. • Only to be disclosed to others on a "need to know" basis.
TRANSFER		
Email	• This information can be sent by email. • No restrictions on emailing information, however it should be limited to a 'need to know' basis. • If appropriate, consider including handling instructions in the email. • When receiving information from an external party you must follow any handling guidance stipulated by the sender or treat it with measures equivalent to Institute requirements. • Where necessary adopt the transmission technique as used by the sender, e.g., encrypting the email. • If you include additional information increasing the sensitivity, consider if a higher classification is required or encryption or password protection.	• To be sent on a "need to know" basis • Insert classification in 'subject' line. • If document is provided by external party, you must originator's lead on encryption when replying to or forwarding emails.
Post (National and International)	• Use clean envelope.	• **DO NOT** mark classification on envelope.

		• Consider using two envelopes and mark the classification on the inner envelope. • Use 'registered' or 'tracked' postal services. • Include a return address on the envelope.
Fax	Faxing should not be considered secure. Please use email as directed above. If fax must be used, ensure documents are marked and the recipient is waiting to receive the fax.	
Printing	Use PIN printing where available. Appropriately dispose of documents once no longer required.	
Photocopying	Use PIN photocopying where available. Only make the number of copies necessary and appropriately dispose of documents once no longer required.	
STORAGE		
Physical storage	• Used in accordance with clear desk / screen policy. • Not to be left on desks or in areas where others may be access it. • Not be left unattended and should be locked away in filing cabinet or draw when not in use or at night. • Laptops must be secured when not in use.	
Electronic storage	• All documents sent or received should be saved with CONFIDENTIAL in the document name. • Appropriate measures should be taken to ensure limited access.	• All documents sent or received should be saved with CONFIDENTIAL-SENSITIVE in the document name. • Appropriate measures should be taken to ensure limited access. • Consider password protecting documents and files.
Digital media, i.e., USB sticks	• Only Institute issued and encrypted media must be used. • Documents should be encrypted. • Documents should be removed as soon as no longer required. • Only delete documents when on Institute premises.	
Disposal of documents	• All marked documents should be disposed of appropriately and in accordance with all regulatory requirements. • Documents should be disposed of securely by using a secure disposal bin or shredding.	
Remote working	• Only encrypted laptops or media should be used when taking Institute information away from Institute premises. • Only take information that is necessary to access whilst away from Institute premises. • Immediately report lost or stolen laptops, media, or mobile phones to your line manager and BICS. Consult the IT Security & Usage Policy.	

Further information is available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf