

## BI-IM-003 INFORMATION CLASSIFICATION & SECURITY POLICY

### Document reference

Policy number:	BI-IM-003		
Policy Owner:	Cass Flowers, Chief Information Officer		
Date:	17 July 2025		
Version:	2.0		
Status:	Active		
EIA number:	BI-IM-003-EIA		
Review period:	3 years		
Last reviewed:	17 July 2025	Next review:	31 August 2028

### Version control

Date	Version	Status	Summary of Changes
01 December 2020	1.0	Archived	Updated in the 2020 Policy Review
20 July 2022	1.1	Archvied	Minor formatting amendments only.
16 August 2023	1.2	Archived	Section 8 added on use of AI Chatbots
17 July 2025	2.0	Active	Policy rewrite to update classification levels and link to Gen AI policy.

### 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
2.0	BEC	N/A	17 July 2025

### Distribution

Date of issue	Version
18 July 2025	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	<input checked="" type="checkbox"/>	Heads of Department	<input type="checkbox"/>
Trustees	<input type="checkbox"/>	BCE Staff	<input type="checkbox"/>

Researcher (Wet)	<input type="checkbox"/>	Nursery	<input type="checkbox"/>
Researcher (Dry)	<input type="checkbox"/>	Visitors	<input type="checkbox"/>
BSU Staff	<input type="checkbox"/>	Credit Card Users	<input type="checkbox"/>
BSU Users	<input type="checkbox"/>	Ionising Radiation Users	<input type="checkbox"/>
Notes: Optional for Trustees			

<b>Associated policies, procedures and guidance</b>
This policy should be read in conjunction with:
BI-IM-002 Data Protection Policy BI-BICS-001 IT Security & Usage Policy BI-IM-004 Generative AI Usage Policy

## Contents

1.	Definitions.....	4
2.	Commitment statement .....	4
3.	Purpose .....	4
4.	Scope .....	5
5.	Classifying data .....	5
5.1.	Security classifications .....	5
5.2.	Descriptors .....	5
6.	Principles.....	6
6.1.	Principle one: Information Value.....	7
6.2.	Principle two: Responsibility and Confidentiality .....	7
6.3.	Principle three: Access Control .....	7
6.4.	Principle four: External Information Handling .....	8
7.	Information handling instructions .....	8
8.	Further information .....	9

## 1. Definitions

<b>“Employee”</b>	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.
<b>“Staff”</b>	Employees and Babraham Institute registered PhD students.
<b>“Individuals”</b>	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), IT Security & Usage Policy (BI-BICS-001) and Generative AI Usage Policy (BI-IM-004).

## 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. Classifying data

### 5.1. Security classifications





- 5.1.1. 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.
- 5.1.2. There are four levels of classification: **Public**, **Internal**, **Confidential** and **Confidential-sensitive** which are outlined in the below diagram 'Information Classification Levels' and referred to throughout this policy.

### 5.2. Descriptors

- 5.2.1. In addition to security classifications, 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]'
- 5.2.2. 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.

## Information Classification Levels

	 <b>Public</b>	 <b>Internal</b>	 <b>Confidential</b>	 <b>Confidential-sensitive</b>
Definition	Unrestricted. May be viewed by anyone inside or outside BI	Restricted to internal personnel and associates	Restricted to a group. May be internal or external	Highly classified and restricted. External access needs strict agreements
Examples	Published research, press releases, official social media	The Hub, meeting notes, newsletters, internal policies	Unpublished research, committee minutes, strategic planning	Personal data, HR records, financial, sensitive research
Handling	No special handling, but maintain accuracy and integrity	Limit access and do not share externally	Shared on a "need to know" basis	Access strictly limited with enhanced security controls
Labelling	Not required, but marked "PUBLIC" if necessary	Marked "INTERNAL"	Marked "CONFIDENTIAL"	Marked "CONFIDENTIAL-SENSITIVE"

## 6. Principles

There are four principles for ensuring appropriate information security that are detailed within this policy. These are summarised below:

## Principles of Information Security



## 6.1. Principle one: Information Value

- 6.1.1. **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.
- 6.1.2. 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 internal, confidential, or confidential-sensitive categories.
- 6.1.3. 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. Principle two: Responsibility and Confidentiality

- 6.2.1. **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.
- 6.2.2. 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.
- 6.2.3. See BI-IM-004 Generative AI Usage Policy for acceptable use of Generative AI tools for work purposes.

## 6.3. Principle three: Access Control

- 6.3.1. Access to confidential and confidential-sensitive information must **ONLY** be granted based on a genuine “need to know” and an appropriate personnel security control.
- 6.3.2. 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.
- 6.3.3. The compromise, loss or misuse of confidential 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.

- 6.3.4. 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.

## 6.4. Principle four: External Information Handling

- 6.4.1. 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.
- 6.4.2. The policy applies equally to assets entrusted to the Institute by others, such as collaborators, commercial clients, and private individuals.
- 6.4.3. 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.
- 6.4.4. 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.

## 7. Information handling instructions

- 7.1. See **Appendix 1** for detailed information handling instructions for each classification.
- 7.2. 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.
- 7.3. 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 or 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 INTERNAL and CONFIDENTIAL-SENSITIVE material must be covered by the higher marking (i.e., CONFIDENTIAL-SENSITIVE).
- Emails 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 email “trail” before they add to it or forward it on.
- Sharing files via OneDrive links is a more secure method than attaching files to an email because you can apply additional security controls. For more information, see [How do I share files in OneDrive?](#)
- 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.

## 8. Further information

- 8.1. This policy will be reviewed regularly to incorporate any changes, legislative or otherwise. The next review date is specified on the cover sheet.
- 8.2. 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.
- 8.3. This policy may be varied, withdrawn, or replaced at any time by the Institute at its absolute discretion.

## Appendix 1 – Information handling instructions

	INTERNAL	CONFIDENTIAL	CONFIDENTIAL-SENSITIVE (to be used in addition to CONFIDENTIAL)
GENERAL			
Legal and statutory requirements must be followed regardless of classification, in particular data protection legislation (UK GDPR and the Data Protection Act 2018).			
<b>Definition</b>	Information restricted to internal staff, students, or associates only and should not be shared externally.	Information restricted to a particular group of people, who may be internal or external to the Institute.	Highly classified information restricted to a small number of people or roles. External access only under strict agreements.
<b>Examples</b>	Internal policies, meeting notes, communications, newsletters, training materials, intranet (The Hub) content, internal project documents	Research data under embargo, contractual documents, unpublished findings, risk assessments, strategic planning documents, committee minutes, non-public policies.	Personal data, HR records, appraisals, sensitive legal or financial documents, H&S / IT incident reports, sensitive areas of research
<b>Handling Summary</b>	<ul style="list-style-type: none"> <li>• Access limited to Institute personnel and authorised associates.</li> <li>• Must not be shared outside the Institute without permission.</li> <li>• Stored in centrally managed / Institute systems.</li> <li>• Should not be accessed in public or insecure environments.</li> </ul>	<ul style="list-style-type: none"> <li>• Shared only on a “need to know” basis.</li> <li>• May be shared externally under appropriate agreements.</li> <li>• Stored and managed in line with centrally managed / Institute systems.</li> <li>• Do not access, read, or discuss in public, open-plan or insecure areas.</li> <li>• Lock away when not in use.</li> </ul>	<ul style="list-style-type: none"> <li>• Requires enhanced security controls.</li> <li>• Must be encrypted when transmitted or stored electronically.</li> <li>• Access strictly limited and logged where possible.</li> <li>• Access strictly limited to those with a verified / approved “need to know.”</li> <li>• Apply additional access controls.</li> </ul>
<b>Labelling</b>	<ul style="list-style-type: none"> <li>• Mark <b>INTERNAL</b> in file header or footer and, if appropriate, include <b>INTERNAL</b> in the file name.</li> </ul>	<ul style="list-style-type: none"> <li>• Include <b>CONFIDENTIAL</b> in the file name and mark <b>CONFIDENTIAL</b> in file header or footer.</li> </ul>	<ul style="list-style-type: none"> <li>• Include <b>CONFIDENTIAL-SENSITIVE</b> in the file name and mark <b>CONFIDENTIAL-SENSITIVE</b> in file header or footer.</li> </ul>

	<ul style="list-style-type: none"> <li>• Apply COMMERCIAL and PERSONAL descriptors if appropriate (see 5.2)</li> </ul>	<ul style="list-style-type: none"> <li>• Apply COMMERCIAL and PERSONAL descriptors if appropriate (see 5.2)</li> </ul>	<ul style="list-style-type: none"> <li>• Apply COMMERCIAL and PERSONAL descriptors if appropriate (see 5.2).</li> </ul>
<b>TRANSFER</b>			
<b>Email</b>	<ul style="list-style-type: none"> <li>• Can be sent internally, but should include a note indicating, e.g. “Internal – Do not forward externally.” Or “Internal use only”</li> </ul>	<ul style="list-style-type: none"> <li>• Information can be sent by email. However, share documents via secure Institute file sharing services (e.g. <a href="#">OneDrive</a>) rather than attaching files to email.</li> <li>• Insert classification in email ‘subject’ line.</li> <li>• Apply additional security controls to shared files, e.g. password protected links, link expiry date, block file download</li> <li>• If appropriate, include handling instructions in the email.</li> <li>• When receiving information from an external party you must follow any handling guidance stipulated by the sender or treat it with equivalent to Institute measures.</li> <li>• Where necessary adopt the transmission technique as used by the sender, e.g., encrypting the email.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>All CONFIDENTIAL rules apply, with heightened caution.</b></li> <li>• To be sent on a strict “need to know” basis</li> <li>• If document is provided by external party, you must follow originator’s lead on encryption when replying to or forwarding emails.</li> </ul>
<b>Post</b>	<ul style="list-style-type: none"> <li>• Use internal mail systems and clearly mark the recipient’s name and location.</li> <li>• Must not be posted externally.</li> </ul>	<ul style="list-style-type: none"> <li>• Hand-deliver to recipient on Campus. Do not send via internal mail.</li> <li>• Use clean envelope if posting externally.</li> </ul>	<ul style="list-style-type: none"> <li>• Hand-deliver to recipient on Campus. Do not send via internal mail.</li> <li>• <u>If posting externally:</u></li> <li>• <b>DO NOT</b> mark classification on envelope.</li> <li>• Consider using two envelopes and mark the classification on the inner envelope.</li> <li>• Use ‘registered’ or ‘tracked’ postal services.</li> </ul>

			• Include a return address on the envelope.
Printing and photocopying	Only print or copy what is necessary. Appropriately dispose of documents once no longer required, e.g. secure bins or shredders.		
STORAGE			
Physical storage	<ul style="list-style-type: none"><li>• Used in accordance with clear desk / screen policy.</li><li>• Store in secure office areas and don't leave documents unattended.</li><li>• Laptops must be secured when not in use.</li></ul>		
Electronic storage	<ul style="list-style-type: none"><li>• Save in secure centrally-managed / Institute systems only (i.e. network file shares, OneDrive, SharePoint / Teams sites)</li></ul>	<ul style="list-style-type: none"><li>• Save in secure centrally-managed / Institute only (e.g. file shares, OneDrive, SharePoint / Teams sites)</li><li>• Restrict access via permissions.</li><li>• Do not transfer to personal devices.</li></ul>	<ul style="list-style-type: none"><li>• All CONFIDENTIAL rules apply, with heightened caution.</li><li>• Password protect files and any sharing links where possible.</li></ul>
Removable media, i.e., USB sticks	<ul style="list-style-type: none"><li>• Only Institute issued and encrypted media must be used, do not transfer to personal devices.</li><li>• Files should be encrypted with a password and removed as soon as no longer required.</li><li>• Only delete documents when on Institute premises.</li><li>• Shred or securely destroy, do not discard in general waste.</li></ul>		
Remote working	<ul style="list-style-type: none"><li>• Access via <a href="#">BI VPN</a> or <a href="#">Microsoft RDS</a> services.</li><li>• Do not download to personal devices.</li><li>• Report any loss or breach immediately.</li><li>• Only take information that is necessary to access whilst away from Institute premises.</li><li>• Immediately report lost or stolen laptops, media, or mobile phones to your line manager and BICS. Consult the <a href="#">IT Security &amp; Usage Policy</a>.</li></ul>		