British Institute of Technology Ltd
Trading As: British Institute of Technology, England (BITE)
Data Protection Policy 2026-27
Owner: Academic Board
Reviewed: 17.07.25
Version: 1.1

Data Protection Policy

1. Introduction and values

1.1. British Institute of Technology (the Institute) needs to process certain Personal Data about living, identified or identifiable individuals such as employees, applicants, students, alumni, customers, research participants and others, defined as Data Subjects in the General Data Protection Regulation (GDPR), to fulfil its objectives and meet legal obligations.

1.2. Such data must only be processed in accordance with this Policy and with the terms of the Institute Records of Processing Activities, which set out the purposes for which the Institute processes personal data.

2. Definitions

2.1. **Processing** is given a broad interpretation in the GDPR: it covers collection, recording, organisation, structuring, storage, retrieval, consultation, use, amending, disclosing, destroying of data, etc. Every person or organisation that holds any personal data about another individual in some form or medium (hard copy or electronic) from where it can be retrieved is 'processing' data.

2.2. **Personal Data** is defined as any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Some examples include addresses, dates of birth, attendance details, comments on coursework, a photo.

2.3. **Special Category Personal Data** is defined as personal data revealing:

a) the racial or ethnic origin of a natural person
b) the political opinions of a natural person
c) the religious or philosophical beliefs of a natural person
d) whether a natural person is a member of a trade union
e) the physical or mental health or condition of a natural person
f) the sexual life or sexual orientation of a natural person
g) genetic, biometric data processed for the purpose of uniquely identifying a natural person

Note 1: the definition of health is considered broadly under GDPR; it is not defined exhaustively but includes information collected in the course of the registration for, or the provision of, health care services; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples, etc. It will also include any information about disability or learning difficulty of a Data Subject.

Note 2: personal data relating to criminal convictions and offences, while not special category personal data, is to be treated with the same safeguards.

2.4. **Data Subject** is the living individual to whom the data relates. For example, for the Institute this would mean each student or member of staff, among others.

2.5. **Data Controller** is the person or entity which, alone or jointly with others, determines the purposes for which and the means any personal data are, or are to be, processed. the Institute, as a corporate legal entity, is a Controller under the GDPR.

2.6. **Data Processor** is any third party which processes personal data on behalf of the Data Controller. For example, this could be a supplier to which some service, such as a payroll, has been outsourced. There must be written agreements with Data Processors to ensure they comply with the GDPR.

2.7. **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 transmitted, stored or otherwise processed. the Institute must have procedures for dealing with such incidents.

3. Purpose

3.1. This Policy sets out the Institute approach to compliance with data protection legislation in respect of its obligations as a Data Controller.

4. Legislative context

4.1. the Institute is required to comply with data protection legislation including the GDPR (U.K. and EU), Data Protection Act 2018 (DPA), Privacy and Electronic Communications Regulations 2003 and other related legislation concerning the processing of Personal Data.

4.2. This legislation sets out a framework of rights and duties which are designed to safeguard Personal Data.

5. Scope

5.1. This Policy and its appendix, as well as other instruction issued, must guide all who process Personal Data in the Institute to ensure that the Principles and responsibilities are followed and any breach, whether deliberate or through negligence, may lead to disciplinary action being taken.

6. Principles

6.1. the Institute must abide by the Principles set out at Article 5 of GDPR, which state that Personal Data shall be:

1) processed lawfully, fairly and in a transparent manner, and shall not be processed unless certain conditions are met;
2) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4) accurate and, where necessary, kept up to date;
5) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which they are processed, and;
6) processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6.2. Personal Data must be processed in accordance with Data Subjects' rights – see clause 8 below.

6.3. Personal Data must not be transferred to a country or territory outside the U.K. or European Economic Area, unless that territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data or a lawful exemption applies.

7. Roles and responsibilities

7.1. Compliance with this Policy is mandatory and disciplinary action may be taken against any member of staff who fails to do so. The accompanying Guidelines should also be followed.

7.2. In order to process data lawfully, the Institute must ensure that a condition from Article 6 (and Article 9, as applicable) of the GDPR is met.

7.3. All users of the Institute personal data must ensure that all such data they process is secured, for example in a locked cabinet or with encryption and by use of confidential waste facilities, to safeguard it from damage or loss and from disclosure to any unauthorised third party in any form either accidentally or otherwise. Please see the Information Security Policies and the appendix below for further details and guidance.

7.4. If the Institute enters into agreements with third parties which include the sharing of personal data it must ensure that adequate protection is offered and will only use the data in accordance with defined purposes, by instigating a written data processing/sharing agreement to cover this.

7.5. As required by the Data Protection (Charges and Information) Regulations 2018, the Institute must pay its annual fee as a Controller to the U.K. Information Commissioner. The Registration reference number is Z8669010.

7.6. All Data Subjects have an obligation to:

- Ensure that any information that they provide is accurate and up to date
- Inform the Institute of any changes to information e.g. contact details
- Inform the Institute of any known errors.

8. Data Subjects' rights

8.1. The GDPR affords Data Subjects a number of rights in Chapter III.

8.2. the Institute must endeavour to comply with any information rights requests made to it by Data Subjects exercising any of these as they apply to the Institute and the particular processing concerned, under the terms laid out in the GDPR, principally at Article 12.

8.3. All such requests should be notified to the Information Governance Team as soon as they are received.

9. Third party access

9.1. There are circumstances, provided for under the DPA, where personal data may be disclosed to third parties without the consent/knowledge of the Data Subject.

9.2. Any such disclosures must only take place if the Institute is satisfied that the party seeking this has provided written evidence of its entitlement/authority to ask for this information and relevant justifications as required, or as the law otherwise allows.

10. Monitoring

10.1. It is sometimes necessary to monitor information, networks and communications, which may include Personal Data. This should be done in line with the Institute Guidelines on the Right to Privacy and the Monitoring of Data. the Institute also operates CCTV and similar equipment to monitor safety and security and prevent and detect crime.

11. Records management

11.1. Regardless of format, Personal Data must only be retained for the length of time necessary to perform the processing for which it was collected.

11.2. the Institute will retain some forms of information for longer than others. Information should be retained in accordance with the Institute Records

Retention Policy and associated Retention Schedule and disposed of securely at the end of retention.

12. Associated information

12.1. Anyone in the Institute processing Personal Data should consider the following checklist:

- Is this data really needed; what is the minimum required?
- Is the data 'standard' or 'special category'?
- What condition(s) for lawfulness of processing is being relied upon?
- Has the Data Subject been informed that this type of data will be processed and the purposes for this?
- Has the Data Subject been informed of his/her rights?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the Data Subject that the data is accurate and current?
- Will the data be securely held and who will have access?
- How long does the data need to be kept and are there arrangements for its review/secure disposal?

12.2. Guidelines are appended to this Policy to advise staff on best practice procedures to follow. These guidelines may be subject to change or revision by the Data Protection Officer or a delegate.

13. Review

13.1. This Policy will be reviewed at least every three years or earlier as required by regulatory changes.

13.2. Minor updates to this Policy that do not affect the rules, principles or intent of this Policy may be made by the Data Protection Officer or a delegate on behalf of the Information Governance Group.

Appendix – Data Protection Guidelines

These Guidelines should be read in conjunction with the Institute Data Protection Policy. Examples are set out below to illustrate some of the scenarios staff might experience and best practice to be adopted.

I. What are my responsibilities?

All staff will process personal data in one form or another and as such have a duty to ensure that this is done in compliance with the Institute policy, such as transparently, fairly and lawfully. As such, all staff should be aware of the **Data Protection Principles** and bear in mind the detailed in the Policy. In particular, be aware of what constitutes special category personal data and the distinct circumstances under which it can be processed. Remember that 'processing' of data has a very broad definition that encompasses collection, storage, transmission, sharing, moving, using, holding, deletion/disposal and so one. Any and all of the below may be applicable to you.

II. Special category personal data

Special category personal data should usually only be recorded when the Data Subject has given explicit consent. There are some exceptions to this listed in Article 9 GDPR such as to protect the vital interests of the individual or another person, to comply with employment law or to monitor equal opportunities.

What to do

When recording data like absences, extenuating circumstances or disciplinary offences on a file, where possible only brief notes should be made with little or no detail e.g. "absent due to ill health".

III. Dealing with Subject Access Requests

Anyone who wishes to make a data Subject Access Request (SAR) should send an email request to info@biot.org.uk, though it is not mandatory and oral requests are possible. Any SAR received within the Institute should be copied to info@biot.org.uk so it can be logged. If in doubt as to whether you have received an SAR or how to respond to it, please contact the Information Governance team for assistance.

the Institute, as Data Controller, must respond to such a request, in full, within one calendar month. There are certain requirements that must be satisfied by the Data Subject before the period for fulfilment begins:

- the person making the request must have properly identified him/herself (if the request is by email it needs to be from a the Institute address or other details verified)
- enough information must be provided to locate the data (i.e. the request must be sufficiently clear as to what is being sought: a Data Subject can't simply say "give me everything you have on me" and expect a full response) *
- there must not have been repeated or similar requests from the Data Subject unreasonably close in time (if so, it may not be necessary to respond)
- there must not be a 'disproportionate effort' involved in responding to the request (although this is a difficult point to argue and the burden is on the Institute to demonstrate this)

* data which may be produced in the event of an SAR is usually to be found in what GDPR defines as a 'filing system'[1]. However, if the request contains a description of the data, the individual would have a right of access to unstructured data. For further details, please use the contact details below.

IV. Fair, lawful and transparent processing of data

When processing personal data, it is important that this complies with the Data Protection Principles. For example, at the point of collection the form, web page or similar should include a privacy/fair processing notice to enable compliance with the first principle and the right to be informed. This should state, concisely and in plain language:

- who the Data Controller is (usually the Institute)
- the purpose(s) for which the data will be processed and the legal basis
- details of any recipients to whom the data may be disclosed/transferred
- retention period or criteria used to determine this
- information on data subjects' rights
- existence of automated decision making and its consequences
- whether provision of data is part of a statutory or contractual requirement or obligation and possible consequences of failure to provide the data

[1] Article 4(6)

For help drafting such a notice please contact the administration department. If you need consent, it is good practice to collect this at this point and keep a record of the consent given as an audit trail.

What to do

Consider the following points when planning a privacy notice:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?
- What is/are the lawful basis(es)?

No data other than that required for that particular transaction should be collected.

V. Information security

Appropriate security measures must be taken when processing data. Personal data should be marked with an appropriate classification as per DG09 – Information Classification Policy and stored and handled (and disposed of) as determined by these. Data is to be given appropriate levels of access control and security. This means that it should be safeguarded by means of lockable cabinets and password and/or encryption protection, depending on format.

Handling and exchange of patient information must in addition comply with the Access to Health Records Act 1990 and the Caldicott principles where only those with a professional or contractual duty of confidentiality are permitted access to patient information.

What to do

Make sure you use passwords which are strong and hard to guess; consider a password manager. Never share or write passwords down and keep a log of who has access to secure areas. Secure personal information physically by restricting access to only those who need it for the performance of their duties and lock cabinets, rooms and computers when the information and device is not in use. Use confidential waste facilities/shredding.

VI. Examinations and assessment data

Students are entitled to information about their marks for all types of assessment, as well as decisions made on academic progress, award and classification. These are normally available as a matter of course but the Institute *may* withhold marks, transcripts and certificates or notification of decisions relating to academic progression or award where a student has tuition fee debts.

However, access to this information is within the provisions of Article 15 GDPR and marks and other data will be released if a subject access request is made (but not in an official format, such as a transcript). Examination scripts (answer books) are exempt from the right of access (Schedule 2 of DPA2018).

- Exam *scripts* are exempt from the right of access (SAR)
- Examiners' *comments* and marks are not exempt and access may be requested

What to do

Markers could make their comments on a separate sheet (although it should be remembered that data must be presented in "an intelligible form" to a Data Subject making an SAR). It is acceptable to destroy the marking sheets/scripts once marks have been finalised at the examination board, if this is part of standard procedure but this should be done in accordance with the Records Retention Policy. In all cases markers should be aware that their comments may be read by the candidate, so offensive, subjective or opinionated statements must be avoided. Please see the current Assessment Handbook for further details, and the ICO's guidance .

VI. (i) Automated decisions

If any form of assessment relies purely on automated means – such as MCQ answers read by a machine – then a Data Subject has the right:

- to be informed of the logic behind the process
- to be able to request that decisions are not made solely through the automated process

VI. (ii) Disclosure of results

- Telephone queries for exam results should not be answered unless there is some verifiable method to confirm the identity of the caller
- Publication of results on a notice board may be reasonably expected by students, but to protect identification, ID numbers should be used rather than names
- Exam results *may* be withheld due to non-payment of fees where the debt relates to academic study

What to do

If exams are not marked until fees are paid, then there will be no data to access. However, this could be argued to be a form of student bias and even infringe human rights. Exam results should be provided if an SAR is submitted but re-enrolment or graduation *could* be prevented. Publishing examination results is a common and accepted practice. Nonetheless, if exam results or

classifications are to be published publicly, such as at a degree ceremony, it is good practice to gain consent or at least offer an opt-out. See also the current Assessment Handbook.

VI. (iii) Examination boards

- A candidate may request access to minutes of examination boards if s/he is referred to, whether by name or some other identifier

- What to do

Board secretaries should ensure that minutes are purely factual. If access is provided, any other individual's details must be redacted unless they have given their consent to the disclosure.

VII. Research

There are specific provisions in GDPR (Article 89) and DPA2018 (Section 19) for the use of personal data in research. the Institute's ethics of research procedures should be studied and complied with.

Before using personal data in research that will be supported by the Institute's facilities, approval should be sought from the Institute's Ethics of Research Committee. As part of the application process the researcher will be required to complete sections on 'Confidentiality, anonymity and data storage' and 'Consent'. Informed consent should be collected from all participants for ethical reasons, although this will not be the legal basis for research. Researchers should adopt a system of anonymous coding (pseudonymisation). Wherever feasible, the minimum data possible and anonymisation should be used.

- Data used for one piece of research can be re-used in other research for a different purpose (see Research Ethics Policy guidelines on secondary use)
- Research data *may* be kept indefinitely
- Research data can be exempted from SAR rules as long as certain criteria are met

What to do

Your research should fulfil all the following criteria:

- the information is to be used *exclusively* for research purposes (includes statistical or historical research purposes) and no other use, not even an incidental one
- the information is not to be used to support measures or decisions relating to *any* identifiable living individual (not just the Data Subject but anyone who may be affected by your research)
- the data must not be used in a way that will cause, or is likely to cause, substantial damage or distress to any Data Subject
- the results of your research, or any resulting statistics, must not be made available in a form that identifies the Data Subjects (unless consented to). For example, if a name of an individual is disguised you would not meet this criterion if you describe their circumstances (such as in a case study) in such detail it may be possible for someone to identify that individual.

All data must be processed in accordance with the Data Protection Principles – there is no blanket exemption.

VIII. References

- Confidential references provided for the purposes of education, training or employment are exempt from the right of access

What to do

Even if references are exempt from the right of access, they could be supplied by the Institute or the external party in a discretionary context. It is therefore important to concentrate comments in references on factual matters (e.g. dates of attendance, duties performed); any subjective observations or academic judgements must be based on fact and personal opinions must be avoided. The author should always indicate how long (s)he has known the individual and in what capacity. As a general rule, you are advised not to include information in a reference that you would not wish the individual concerned to see. Spent disciplinary sanctions must not be referred to (usually six years after case closure). Personal references should be limited to a maximum of six years after the student or member of staff leaves the institution.

Nonetheless, students would not normally object to the confirmation of attendance, degree classifications etc. which come from prospective employers (NB this type of enquiry could be treated as an FOI request). Likewise, references may be requested by new prospective employers of current or ex-staff. References provided in a personal capacity by staff should state this clearly and not be provided on the Institute stationery.

IX. HR records

IX. (i) Disciplinary procedures

- The outcome of grievances is only disclosable to the person who is the subject of the process, not to any other parties

What to do

If there is a disciplinary process against an employee, then only that employee has a right to know the details of that process. For example, if an accusation is made by a student or member of staff against another member of staff, expectations should be managed from the start. The accuser does not always have a right to be kept informed or to know the outcome of the process; however, if staff or student safety is involved in relation to a case, then the minimum information necessary will be provided to complainants in relation to a case outcome. Otherwise, only confirm that the procedure has been completed when it has, but not how. This will need to be carefully determined depending on the nature of the case.

IX. (ii) Fitness to work/'sick' notes

- Fit notes contain special category personal data and should only be seen by those who *need to know*

What to do

These notes should not have to be seen by line managers unless explicit consent has been given by the employee.

X. Images

Images of identifiable individuals are personal data.

- Photos/video taken for official use are covered by data protection legislation and people in them should be advised why they are being taken and how they will be used
- Photos/video showing a crowd scene (e.g. in a public place) would not be considered to be

personal data because the purpose of capturing the individuals is not to identify them

- Photos of staff on websites accessible to the Internet require consent. If a site is intranet only consent isn't necessary, but staff cannot be forced and it is good practice to offer an opt-out

What to do

Consent should be sought wherever possible, especially of individual shots because they can be readily identified. Where this is not practical for each individual, for example at an event or at a degree ceremony, Data Subjects should be made aware so that it is within their expectations: a statement should appear on tickets/programmes and/or a notice be displayed explaining that photographs/video are being taken and the purpose to which these may be put. All photographers should be clearly identified, e.g. with a visible badge. If taking photographs of children, consent must be obtained from a parent or guardian.

If a student or member of staff objects to having a photograph published, on a departmental website for instance, then it must be removed. Prior consent should be sought wherever possible.

External Relations can provide a photo/video release form which Data Subjects should sign if their photo will be used in a the Institute publication or website.

In addition, individuals whose image has been recorded by CCTV have a right of access to a copy of those images by making a subject access request. This is covered by the Institute's CCTV Policy.

XI. Direct marketing

- Data Subjects have the right to ask organisations to stop, or not to start, direct marketing aimed at them

What to do

It is accepted that, for example, alumni might reasonably expect the Institute to send a variety of mailings to them. However, alumni (or anyone else receiving direct marketing material) should be advised of their rights and given the opportunity to opt out in every communication.

Any recipients of direct marketing should be asked to opt in to receiving such communications. Staff should be aware of the need to comply with the Privacy and Electronic Communications Regulations.

XII. Third parties, outside agencies and international processing

It can be a serious offence to disclose any personal data to a non-authorised person, including orally. It can usually only be released with the Data Subject's consent, unless one of the exemptions from DPA2018 is met or a court order issued.

- When dealing with a third party acting as a Data Processor

What to do

A number of third parties process personal data on the Institute's behalf under our instructions. It is important to ensure that a written agreement is in place covering the services the third party is to provide and that it includes specific provisions covering its responsibilities for the personal data it processes (e.g. an obligation to assist the Institute in responding to an SAR) and references data protection legislation. Ideally the third party should provide an indemnity covering any penalties the Institute might suffer as a result of their use of the data. Note that there exists a Personal

Information Sharing Agreement between the Institute and the Students' Union, which is a separate Data Controller.

- When personal data may be transferred outside the U.K./EEA

What to do

Personal data may be passed to partnering organisations in countries outside the EEA, such as BUPT, which do not have the same levels of protection for personal data as long as certain safeguards are in place (though there are some exemptions). Data Subjects must be informed prior to any transfer. Details of these safeguards, derogations and of standard contractual clauses which may be employed are available from the Records & Information Compliance Manager. See also section XIII. below.

- Individual enquiries e.g. from friends or relatives in person, by telephone, email etc. need to be handled with care

What to do

The correct procedure is to pass any message on to the Data Subject and leave it up to them to contact the caller. Even if the message is from an apparently anxious parent, there is no requirement to reveal details or even confirm the Data Subject exists! If an enquirer telephones (or emails from a non-the Institute account) and claims to be the Data Subject, to provide some measure of authentication, offer to call back. Otherwise there needs to be some system of security questions/passwords to confirm the identity of the caller. Note that a sponsor or parent does not have any automatic right to a student's marks or progression details without the consent of the student, even if the student is under 18.

- Enquiries from the police or other crime prevention or law enforcement organisations (or revenue-collecting authority)

What to do

These requests most commonly come from the police but *may* also come from an investigation in to tax/benefit fraud or immigration e.g. from local government or the UKVI. The agency must complete a Schedule 2 Part 1 form (available on request) to apply for access specifying the purposes for which it is required. The data must be necessary, not just helpful to these purposes. Even then, the Institute is not compelled to release the data: there is a need to ensure proportionality, so rights and interests should be balanced in coming to a decision. It's important to verify the identity of anyone making such requests and ensure the request is counter-signed by an authorised individual. This should be someone who is senior in rank/position to the requester.

- Protecting the vital interests of the Data Subject or preventing serious harm to a third party

What to do

The consent of the Data Subject is not required if a failure to release data would result in her or a third party's harm or if required to perform a regulatory function, such as securing health and safety at work.

XIII. What other possible exemptions are there to the release or other processing of personal information?

- Data protection legislation does not cover the deceased
- Data may be released to the police or other law enforcement organisation in pursuit of an active investigation (see XII. above)
- Disclosure of data may be necessary in the case of a medical emergency to protect someone's life (vital interests lawful basis)
- the Institute is legally obliged to pass certain data to certain third parties such as HESA/JISC, OfS, HMRC, etc. (legal obligation lawful basis)

XIV. What are the penalties for Data Controllers if they breach the law?

- Fines can be issued for breaches of GDPR as set out at Article 83
- Depending on the nature of the infringement, circumstances and severity, these fines can be up to €10m or 2% of worldwide annual turnover or up to €20m or 4% of worldwide annual turnover, in both cases whichever is higher
- Criminal prosecutions may be brought against not just the directors or trustees of an organisation but also other officers (i.e. employees) who are responsible for a breach. This personal liability is important to note
- A Data Subject can bring a claim for compensation for a breach and not necessarily just those that may have resulted in their suffering damage or distress
- The Information Commissioner may serve an enforcement notice on a Data Controller if an investigation results in a finding that one of the data protection principles has been breached. The ICO sets out the remedial steps which need to be taken by the Data Controller in question and failure to comply with these instructions would also be a serious offence under the DPA2018

XV. Who has the authority to report any breaches?

Any personal data breaches must be reported to the Information Governance Team. Any (suspected) breaches will be considered for notification to the ICO as the GDPR imposes a duty on all organisations to report certain types of breach within 72 hours of becoming aware of it, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the Institute must also inform those individuals without undue delay.

XVI. Who in the Institute can I contact for more advice?

The advice above is not exhaustive. The Information Governance team can be contacted by emailing info@biot.org.uk including to arrange training.