BLOOMSBURY INSTITUTE LONDON

Data Protection Policy

Index

Document Version Control

Document Version	Committee	Committee Action	Date
	SMLT	Recommend approval	08 September 2021
	Board of Directors	Approved	13 September 2021
V2.0		**Date in force**	**13 September 2021**

This Data Protection Policy will be reviewed annually by our Senior Management and Leadership Team (SMLT). A review may also be triggered because of changes in the legislative requirements. Any amendments will be subject to approval by the Board of Directors.

1. Policy statement

This policy is a statement of the measures which Bloomsbury Institute has adopted to ensure it is compliant with relevant data protection legislation.

Bloomsbury Institute undertakes to apply this policy to all persons associated with Bloomsbury Institute with regard to the delivery of Bloomsbury Institute courses. In this context, 'all persons associated with Bloomsbury Institute encompasses all staff, students, accredited visitors (for example guest speakers), and any person acting as a Data Processor on behalf of Bloomsbury Institute. [See below for a definition of a Data Processor]. This captures potential staff and students (applicants), current staff and students, and former staff and students.

This policy is designed to ensure Bloomsbury Institute's full compliance with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

The overarching principles of this policy apply to our IT and electronic systems. Data protection in the context of IT systems is also supported by a suite of separate policies and regulations which cover IT systems and their use.

2. Legal Framework

The legal framework for data protection in the UK is provided by the Data Protection Act 2018 which recognises Article 8 of the European Convention on Human Rights 1950 in relation to the "right to respect for one's private and family life, his home and his correspondence", essentially personal privacy. The UK GDPR sits alongside the Data Protection Act 1998 to ensure the consistency of data protection standards at an international level. This has become crucial given that personal data is increasingly being stored, processed and exchanged on the internet and as such often exists in an international environment.

The Data Protection Act 2018 has served to empower individuals to take control of their personal data by assigning them rights over their personal data and protecting them from the erroneous use of that same data. The Data Protection Act 2018 also imposes responsibilities and requirements on any organisation that handles personal data, requiring them to comply with a number of important principles and legal obligations.

The Information Commissioner's Office (ICO) is the supervisory authority for data protection in the UK. It offers advice and guidance, promotes good practice, monitors breach reports, conducts audits and advisory visits, considers complaints, monitors compliance and takes enforcement action where appropriate. The ICO can be contacted at https://ico.org.uk/make-a-complaint/. Bloomsbury Institute's registration number is **Z1082474** and further details of the Data Protection register entry can be found on the Information Commissioner's public register which can be found here[1].

Included within Appendix A is a set of definitions for key terminology in relation to data protection.

3. Scope

This policy applies to all personal data we process about Data Subjects, regardless of the location of where that personal data is stored. This policy applies to all staff, working on or off campus, and others processing personal data as a part of their role and remit. Failure to comply with this policy may result in disciplinary action for staff at Bloomsbury Institute.

All Heads of Divisions/Departments and Directors, which are office holders of functional areas, are responsible for ensuring that respective staff within their area of responsibility comply with this policy and should develop appropriate practices, processes, controls and training to ensure that compliance is met.

[1] https://ico.org.uk/ESDWebPages/Search

The Data Protection Officer (DPO) is responsible for overseeing this policy. The DPO can be reached at dpo@bil.ac.uk.

4. The Data Protection Principles

The Data Protection Principles by which all processors of personal data must abide are set out in Article 5 (1) of the UK GDPR. These principles form the basis for the Data Protection Act 2018. Any processing of data which breaches one or more of these principles is unlawful.

The Data Protection Principles are as follows:

4.1 Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

For data to be processed lawfully, one of the legal bases set out in Article 6 of the UK GDPR must also apply. See Appendix B.

To ensure compliance with this first principle, we set out clearly and publicly within our Privacy Notice[2] how we will collect, use and share a student's data be they past, present or prospective students and for what purpose. The same Notice seeks to help students understand their rights in relation to the personal data we hold. This ensures that they are in a position to make an informed decision about whether or not to provide the data requested. Compliance with this principle is also ensured through staff training.

4.2 Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

We will only process personal data for the specific purposes explained to the data subject at the point of collection. This means that we will not collect personal data for one purpose and then use it for a different and unrelated purpose. Should we need to use the data for a different and unrelated purpose, we will inform the data subject of the new purpose before any processing takes place. In some cases, we may require the consent of the data subject.

For archiving purposes that are in the public interest, scientific or historical research purposes or statistical purposes, further processing of data beyond its original stated purpose is not considered to be incompatible with the initial purposes. In such cases, we are not required to notify or seek the consent of the data subject.

4.3 Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they were processed.

This means that we will collect or process only the minimum amount of personal data we need to properly achieve the purpose in question. Information which is not needed or is not relevant for a purpose will not be collected or otherwise processed.

Whenever possible, personal data should be anonymised or pseudonymised at the earliest opportunity.

[2] Bloomsbury Institute's Privacy Notice is available from Section 3 of its online Quality and Enhancement Manual, and is made available to the student at the point the data is being collected.

4.4 Accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

In order to be accurate, data has to be both correct and clear in terms of meaning. For that reason, we will check the accuracy of any personal data at both the point of collection and at regular intervals afterwards.

As far as possible, personal data based on facts must be distinguished from personal data based on personal assessments. An additional distinction to be made, where relevant and possible, is between different categories of data subjects e.g. those suspected of having committed a criminal offence, those who may be the victims of a criminal offence, and those with information about a criminal offence.

We will correct or erase any inaccuracies, as appropriate, although we will not delete information if it has been used to inform decisions affecting a data subject. In such cases, we will correct the information for future use (so as to ensure it is up to date) and add an explanatory note on file to explain the situation. Where a data subject disagrees with a professional opinion about him or herself which does not – by definition – constitute verifiable fact, the data subject's difference of opinion will be noted on the file in the relevant places.

We will not transmit any data we are lawfully permitted to transmit without first verifying the quality of the data. This means we will not transmit any data that is inaccurate, incomplete or no longer up to date. Should we fail to do so, we will notify the recipient immediately.

4.5 Storage limitation

Personal data must be 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 if the personal data is to be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

This means that we will destroy (securely) or erase data from our systems when there is no longer a legal, business or operational requirement for us to retain it, taking into account the purposes for which we originally requested it. We will not retain personal data "just in case" we think it might prove useful at some future date. Our Data Protection Officer will advise on periodic reviews based on our data retention schedule which can be found in the Student Records Policy[3].

4.6 Integrity and confidentiality (Security)

Personal data is 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. Organisational measures to safeguard security include training.

4.7 Accountability

The Data Controller must be responsible for, and be able to demonstrate, its processing activities are compliant with the Data Protection Principles.

Bloomsbury Institute must implement appropriate technical and organisational measures to ensure compliance with the data protection principles. The institution must be able to demonstrate compliance with, the data protection principles. Bloomsbury Institute staff, contractors and authorised third parties who process personal data on the Institution's behalf will give effect to this policy through complying with it along with related policies, procedures and processes.

[3] https://www.bil.ac.uk/qem/policies/

We have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

- a suitably qualified Data Protection Officer (DPO);
- adopting a Privacy by Design approach when processing personal data and completing a data protection impact assessment where processing presents a high risk to the privacy of data subjects;
- integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, records of processing and records of personal data breaches;
- annual training staff on compliance with Data Protection legislation and keeping a record accordingly;
- regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

5. Data protection by design and default

Data protection by *default* is linked to the fundamental protection principles of data minimisation and purpose limitation whereby we are required to ensure that personal data is processed with the highest privacy protection and not made accessible to an indefinite number of persons.

Data protection by *design* is the practice of anticipating and embedding data protection measures within any project (e.g. collecting a new type of data or implementing a new system or process for holding or accessing personal data) from the outset. This ensures that security is a key consideration rather than an after-thought. Data protection by design is closely linked with the requirement for record keeping and accountability.

The UK GDPR includes the following specific obligations in relation to data protection by design:

- **Information Security** should be considered at all stages and must be appropriate to the risk involved.
- **Data sharing** and in particular international data transfers, must be subject to careful consideration to ensure that it is lawful.
- **Data Protection Impact Assessments**, which are required when a data processing activity is likely to result in a “high risk” to the rights and freedoms of data subjects.
- **Data Protection Officers (DPO)** may need to be appointed by some organisations.
- **Privacy policies / Information Notices** which help ensure transparency by requiring data controllers to provide certain information to individuals.

6. Data subject rights

The UK GDPR sets out eight data subject rights with which we are required to comply. The only exception is in relation to the use of personal data in research[4] where these rights can be restricted.] These rights are listed below.

[4] Personal data in research may only be collected after approval by our Research Ethics Committee.

6.1 The right to be informed

Individuals have the right to clear and concise information about what we plan to do with their personal data. We are required to provide this information before we use their data; hence the Privacy Notice[5] that we make publicly available on our website.

6.2 The right to subject access

Individuals have the right to request to see or receive copies of any information we hold about them and to be assured that the processing of their data is fair and lawful. Such requests must be referred to our Data Protection Officer who will ensure a response is provided to valid requests within one month of receipt. No such rights exist, however, in relation to exam scripts and exam marks.

Staff and students have the right of access to information which is kept about them in both electronic and manually held files. Any person wishing to exercise this right should make their request in writing to the DPO. When making such a request, referred to as a Subject Access Request, the individual must:

- Provide a suitable means of identification.
- Inform the Data Protection Officer where they believe the information is held.

Although individuals are able to obtain a copy of their personal data free of charge, we are entitled to charge for any additional copies. We are only able to charge a fee if we think the request is manifestly unfounded or excessive. If so, it would be reasonable for us to charge a fee for administrative costs associated with the request.

Bloomsbury Institute undertakes to:

- Ensure that no decisions that affect the individual concerned are based solely upon an automated decision-making process or incorrect information.
- Prevent processing likely to cause damage or distress.
- Prevent processing for the purposes of direct marketing.
- Act to rectify, block, erase or destroy inaccurate data.
- Ask the Information Commissioner to assess whether any part of the Data Protection Act 2018 has been contravened.

6.3 The right to rectification

If personal data is inaccurate, data subjects have the right to require us to rectify inaccuracies. In some circumstances, if personal data is incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement. We will assess the request and correct any inaccuracy.

6.4 The right to object

Individuals have the right to object to specific types of processing such as processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right. We will assess the request and respond accordingly.

[5] https://www.bil.ac.uk/qem/policies/

6.5 The right to erasure

In certain circumstances data subjects have the right to have their data erased. This only applies:

- where the data is no longer required for the purpose for which it was originally collected or processed, or
- where the data subject withdraws consent, or
- where the data is being processed unlawfully.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to make achievement of that processing impossible or disproportionately difficult
- for the establishment, exercise or defence of legal claims

We will assess the request against the criteria in Article 17 of the UK GDPR and respond accordingly.

6.6 The right to portability

Individuals have a right to obtain and reuse their personal data across different services. This includes a right to have that data provided in a structured, commonly used and machine-readable format so it can be forwarded to another data controller. This only covers data submitted to us by the subject or data we have captured on the subject's use of a service, for example, use of online services like our VLE, where we might see time spent on the VLE, number of logins by a student during a given period of time etc. If technically possible, we will consider transferring information directly to another organisation.

6.7 The right to restrict processing

In some circumstances, data subjects may not wish to have their data erased but rather have any further processing restricted. In these circumstances we might move the data to another processing system or simply make the data unavailable to users.

This right is not absolute and only applies if:

- the individual contests the accuracy of their personal data and we are verifying it
- the data has been unlawfully processed i.e. in breach of the 1st Data Protection Principle, and the individual does not want it erased
- we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim
- the individual has objected to us processing their data under Article 21 of the UK GDPR, and we are considering whether our legitimate grounds override those of the individual

6.8 The right to automated decision-making and profiling

In the case of automated decision-making and profiling that may have significant effects on data subjects, data subjects have the right to either have the decision reviewed by a human being or to not be subject to this type of decision-making at all. These requests must be forwarded to the Data Protection Officer immediately.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

7. Notification

Bloomsbury Institute is registered as a Data Controller and a Data Processor and has notified the Information Commissioner of:

- The personal data it holds
- The personal data that it will process.
- The categories of data subjects to which personal data relates.
- The purposes for which the personal data will be processed.

If processing for a new or different purpose is introduced the individuals affected by that change will be informed and the official notification will duly be updated to reflect the said change.

8. Responsibilities of staff and students

Staff at Bloomsbury Institute are responsible for:

- Ensuring that any information provided to Bloomsbury Institute in connection with their employment is accurate and up to date.
- Informing Bloomsbury Institute of any errors or changes to information which they have provided (e.g. change of address).
- Checking the information Bloomsbury Institute sends out from time to time giving details of information kept and processed about staff.
- Correct processing of data during the course of their employment.

Staff at Bloomsbury Institute who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy and must ensure that:

- all personal data is kept securely.
- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party. If staff are unsure to whom they can legitimately disclose personal data, they can seek advice from the DPO.
- personal data is kept in accordance with our retention schedule.
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO.

- any data protection breaches are swiftly brought to the attention of the DPO and that they support the DPO in resolving those breaches.

- where there is uncertainty around a data protection matter, advice is sought from the DPO.

Where members of staff are responsible for supervising students doing work which involves the processing of personal information (for example in research projects), they must ensure that those students are aware of the Data Protection Principles.

Students must likewise ensure that they are familiar with the Privacy Notice[6] provided by us and ensure that any information they provide to Bloomsbury Institute is kept up to date.

Where external companies are used to process personal data on our behalf, responsibility for the security and appropriate use of that data remains with Bloomsbury Institute.

Where a third-party data processor is used:

(a) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;

(b) reasonable steps must be taken that such security measures are in place;

(c) a written contract establishing what personal data will be processed and for what purpose must be set out;

(d) a data processing agreement must be signed by both parties.

9. Security

It is of the utmost importance that data is kept securely particularly special categories of personal data. Precautions must be taken against physical loss, damage to or corruption of data. Our Information Security Policy supports compliance around the 'integrity and confidentiality' principle of the regulation in ensuring appropriate technical measures are in place to protect personal data. All staff should ensure that any personal data, which they hold, is kept securely and that personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. It is essential to protect the security and confidentiality of data during storage, transportation, handling and destruction. The transportation of personal data in any format (laptop, hard copy) should be avoided.

All personal information in the form of manual records should be kept in a locked filing cabinet or kept in a locked drawer in a lockable room where access is limited to relevant staff only.

If information is computerised, it should be password protected, with passwords being changed regularly so that only authorised people can view or alter confidential data.

Personal data must not be transferred outside of the European Economic Area (EEA), including the use of websites or applications hosted on servers based outside of the EEA, unless appropriate safeguards are in place.

Key to security is staff training. Bloomsbury Institute is committed to ensuring its staff have the requisite training and awareness around data protection. All staff must undertake the compulsory data protection training, cyber security awareness training and other training as required.

Any breach of data protection law due to unauthorised access, misuse or loss may result in disciplinary action, up to and including dismissal.

[6] https://www.bil.ac.uk/qem/policies/

10. Vendors, contractors, and suppliers

Vendors, contractors and suppliers are often required to have access to areas in which personal data may be stored or processed. It is therefore necessary to ensure they are:

- Controlled, documented, and are wearing some form of identification.
- Restricted from unnecessary admittance to areas where personal data is held or processed.
- Required to sign nondisclosure agreements where access to personal data is unavoidable.

11. Disclosing personal data

Personal data should not generally be disclosed to third parties without the permission of the individual concerned. In this context "third parties" includes but is not limited to student recruitment agents, family members, friends, local authorities, government bodies, the UK Visas and Immigration (UKVI), and the police, unless disclosure is exempted by the Data Protection Act 2018 or by other legislation. The Data Protection Act 2018 sets out the following circumstances in which data may be released without the express consent of the individual:

- For the purpose of protecting the vital interests of the individual (e.g. release of medical data where failure to do so could result in harm to, or the death of, the individual).
- For the prevention or detection of crime.
- For the apprehension or prosecution of offenders.
- For the discharge of regulatory functions, including securing the health, safety and welfare of persons at work.
- Where the disclosure is required by legislation, by any rule of law or by order of a court.

12. Disposing of personal data

We are required to retain certain records for operational and administrative purposes and to demonstrate compliance with statutory or regulatory requirements. This is done while remaining compliant with the Data Protection Principle which requires that personal data are not kept longer than is necessary for their purpose.

The Data Protection Act 2018 places an obligation on Bloomsbury Institute to err on the side of caution when disposing of personal data. All staff have a responsibility to consider safety and security aspects when disposing of personal data in the course of their work. Consideration should also be given to the nature of the personal data involved (how sensitive it is), and the format in which it is held.

Staff should ensure that all paper or microfilm documentation containing personal data is permanently destroyed by shredding or incinerating it, depending on the sensitivity of the personal data. If there are any details of a private nature on a piece of paper, this paper must be disposed of in the correct manner to ensure that it cannot be reconstituted, and the data stolen. This means shredding it.

13. Collection and processing of personal data relating to disability

Bloomsbury Institute will often collect student disability information at the admission stage, but collection of disability data may also occur throughout the period of study. Bloomsbury Institute will provide:

- Mechanisms to ensure that where disability data is provided for a stated purpose, such as to ensure adequate service provision, it is not misused for other purposes, such as to make a decision about whether or not to admit a student to a course of study.

- A system whereby when there is a need to disclose disability data to external organisations, prior consent of the Data Subject should be obtained for each disclosure. The data subject should be informed about the nature of the information to be disclosed, the intended recipient, and the purpose of disclosure should be given to the data subject. This is done by the use of a "consent to share form".

14. Compliance

Bloomsbury Institute is responsible for ensuring that their staff receive appropriate training in the collection, processing and management of personal data. However, all staff have a personal responsibility for compliance with data protection legislation as set out in this policy.

Any breach of data protection and confidentiality[7] could have severe implications for Bloomsbury Institute, our students and staff. See Section 15 below. Consequently, any breaches of confidentiality or unauthorised disclosure of any information subject to the Data Protection Act 2018 will constitute a serious disciplinary offence under Bloomsbury Institute's Staff Disciplinary Procedure[8].

In addition to the above ongoing compliance requirement, all staff are required to report any actual or suspected breaches of confidentiality or other incidents including "near misses" to the Data Protection Officer as a matter of urgency. This will allow for a quick response in terms of both addressing the breach and meeting our external reporting obligations. The Data Protection Officer is then responsible for logging, investigating and responding to all reported incidents. The Data Protection Officer is also responsible for reporting all serious breaches to the Information Commissioner's Office within 72 hours. It is also the responsibility of the Institution as data controller to make a report to the ICO in cases where a third party is processing data on its behalf. Where a breach is likely to result in a high risk to the rights and freedoms of a person, the Institution as data controller may be required to report the breach to the person in question.

The Data Protection Officer is responsible for deciding whether a report should be made to the ICO and/or to the person in question, and for communication of the relevant information as required.

15. Enforcement

Certain breaches of the UK GDPR and Data Protection Act 2018 are criminal offences for which both individuals and organisations can be prosecuted. However, the most common action taken by the ICO for breaches is to issue Enforcement Notices which require organisations to take specified actions to ensure they comply with the law. For serious breaches of the UK GDPR, the ICO can serve administrative fines of up to 4% of annual global turnover or £17.5 million – whichever is the greater.

[7] Examples of breaches include loss or theft of data or equipment, ineffective access controls allowing unauthorised use, equipment failure, unauthorised disclosure (e.g. email sent to the incorrect recipient), human error, and a hacking attack.

[8] https://www.bil.ac.uk/qem/

16. Record keeping

Under the UK GDPR, we are required to keep full and accurate records of all our data processing activities, including records of data subject consents and procedures for obtaining consents where consent forms the legal basis of processing. These records should include the following:

- The name and contact details of the institution as a Data Controller and the Data Protection Officer
- Clear descriptions of
  - the personal data types we collect
  - the processing activities with which we engage
  - processing purposes
- Any third-party recipients of personal data
- Personal data storage locations
- Personal data transfers
- The retention schedule for personal data
- A description of the security measures in place for personal data including special categories of personal data.

In addition, we are required to keep records of all personal data breaches which include details of the circumstances surrounding them and the remedial action taken.

17. Making a complaint

We are committed to ensuring that all personal data for which we are responsible as a Data Controller is handled in accordance with the legislative framework within which we operate. However, if you have any concerns or complaints about our handling of personal data, then please contact our Data Protection Officer at: dpo@bil.ac.uk.

All data subjects also have the right to make a complaint about our handling of personal data to the Information Commissioner's Office and can do so here[9].

18. Equality Statement

This policy reflects the provisions set out in the Equality Act 2010 so as to ensure that no one receives less favourable treatment on the basis of the protected characteristics of their age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex (gender) or sexual orientation. In addition, this policy is designed to ensure human rights are respected and protected.

19. Further advice and guidance

Further advice and guidance can be obtained from our Data Protection Officer - dpo@bil.ac.uk.

[9] https://ico.org.uk/make-a-complaint/

20. Related regulations, policies and procedures

External

- Computer Misuse Act 1990
- Data Protection Act 2018
- Equality Act 2010
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998

Internal

- Anti-virus Policy
- Computer Use Regulations
- Email Acceptable Use Policy
- Information Control Procedures
- Information Security Policy
- Internet Acceptable Use Policy
- CCTV Policy
- IT Disaster Recovery Plan
- Network Policy
- Password Policy
- Privacy Notice
- Research Ethics Code of Practice
- Social Media Communications Policy
- Staff Disciplinary Procedure
- Student Complaints Policy and Procedures

21. Review of Bloomsbury Institute Data Protection Policy

This Data Protection Policy will be reviewed annually by our Senior Management and Leadership Team (SMLT). A review may also be triggered because of changes in the legislative requirements. Any amendments will be subject to approval by the Board of Directors.

Appendix A: Definitions

1. Personal Data

Personal data means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an address, a student number, an IP address, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data may also include special categories of personal data. Such data includes sensitive data e.g. data relating to race/ethnicity, political, philosophical and religious opinions/beliefs opinion, trade union membership, health (both physical and mental health), sexual orientation, sex life, and genetic data or biometric data. These are considered to be more sensitive and may only be processed in more limited circumstances.

Personal data also includes an expression of opinion about a person (e.g. performance appraisal or comments on scripts), and an expression of the intentions of other people including our own institution towards them. It also includes any numerical or statistical information (e.g. financial information, assessment information) from which an individual's identity can be derived either directly or indirectly from a combination of data.

Personal data relating to criminal convictions (actual or alleged) is **not** classed as special category data, but must be treated in a similar way.

Personal data may be held or stored in many different ways for example on paper or electronically in computers, smartphones, cameras and CCTV, webpages, voice recordings or removable media such as external hard drives, flash drives, CDs and DVDs. It can also be exchanged in many ways including by email, SMS (text message), telephone, and in conversations or meetings. The Data Protection Act 2018 and UK GDPR extend to all such information and formats of information.

Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

2. Anonymisation and Pseudonymisation

If personal data can be truly anonymised, then the anonymised data is not subject to data protection legislation. If this is not possible, it is advisable from a good practice perspective to aim for partial anonymisation or pseudonymisation of data. Pseudonymisation involves the separation of personal data from direct identifiers so that no connection to an individual can be made without additional information that is held separately. Although partially anonymised and pseudonymised data are not exempt from data protection legislation, we recognise that they provide an added layer of security for the handling and processing of data.

3. Data Controller

The Data Controller is the individual/organisation registered with the Information Commissioner who is responsible for ensuring compliance with the requirements of the Data Protection Act 2018 and UK GDPR. This includes determining the purpose(s) for which personal data are collected and processed, and the means by which that data is processed. The Data Controller is ultimately responsible for the personal data, whether it passes the data to a Data Processor or not. Examples of data processors include Canvas and Turnitin. Bloomsbury Institute is the Data Controller.

4. Data Processor

A Data Processor is any individual or organisation who processes personal data on behalf of – and according to the purposes defined by – the data controller.

5. Data Protection Officer (DPO)

Data Protection Officer (DPO) is the person appointed as such under the UK GDPR and in accordance with its requirements. A DPO is responsible for advising the Institution (including its employees) on their obligations under Data Protection Law, for monitoring compliance with data protection law, as well as with the Institution's polices, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.

6. Data Subject

The Data Subject is an individual who is the subject of personal data. This will include staff, current and prospective students, former students, suppliers of goods and services, business associates, etc.

7. Processing

Processing means collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, making available, aligning or combining, deleting data and anything else which can be done with data. A Data Processor is, therefore, any individual or organisation who processes personal data on behalf of the Data Controller according to the purposes defined by the Data Controller.

8. Filing System

Filing System means any structured set of personal data which are accessible according to specific criteria (e.g. student name, student number), whether centralised, decentralised or dispersed on a functional or geographical basis; paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible: i.e. structured by reference to individuals (e.g. alphabetical), by reference to criteria relating to individuals, by numerical reference (e.g. student number) etc.

Appendix B: The lawful bases for processing any personal data

The lawful bases for processing personal data are set out in Article 6 of the UK GDPR. At least one of these conditions must apply when processing personal data:

1. Consent

The individual has given clear consent for us to process their personal data for a specific purpose.

It is important to note that consent must be freely given, specific, informed, and unambiguous. Consent must also require a positive opt-in. It is not acceptable to use pre-ticked boxes or any other method of default consent.

2. Contract

The processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

3. Legal obligation

The processing is necessary for us to comply with the law (not including contractual obligations).

Regulatory requirements also qualify as a legal obligation for these purposes where there is a statutory basis underpinning the regulatory regime and which requires regulated organisations to comply.

4. Vital interests

The processing is necessary to protect someone's life.

5. Public task

The processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

The public task basis will cover, inter alia, processing necessary for:

- the administration of justice;
- parliamentary functions;
- statutory functions;
- governmental functions; or
- activities that support or promote democratic engagement.

6. Legitimate interests

The processing is necessary for our 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.

Legitimate interests is the most flexible lawful basis for processing. The legitimate interests can be either our own interests or the interests of a third party. They can include commercial interests, individual interests or broader societal benefits. In considering legitimate interests we clearly need to balance our interests against the individual's. If the individual would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override our legitimate interests.

The processing must be necessary. If we could be expected to reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.

Appendix C: The lawful bases for processing special categories of personal data

The lawful bases for processing special categories of data are set out in Article 9 of the UK GDPR and supplemented by additional conditions and safeguards set out in the Data Protection Act 2018. At least one of the conditions set out in Article 6 of the UK GDPR (See Appendix A) and one of the following conditions set out in Article 10 of the UK GDPR must be met when processing special categories of data:

- The data subject has given explicit consent.
- The processing is necessary for the purposes of employment, social security and social protection law.
- The processing is necessary to protect someone's vital interests (either the data subject or another natural person) where the data subject is physically or legally incapable of giving consent
- The processing is manifestly made public by the data subject.
- The processing is necessary for legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, the provision of health or social care or treatment or the management of health or social care systems and services.
- The processing is necessary for public health.
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards.