# Data Protection and Confidentiality Policy

BLOOMSBURY
INSTITUTE
LONDON

# Index

# Document Version Control

| Document Version | Committee | Committee Action | Date |
|---|---|---|---|
| 4.0 | SMT | Recommended approval | 5 July 2023 |
| | Board of Directors | Approved | 21 July 2023 |
| | | **Date in force** | **1 August 2023** |
| 5.0 | SMT | Recommended approval | 8 May 2024 |
| | Board of Directors | Approved | 3 June 2024 |
| | | **Date in force** | **4 June 2024** |
| 6.0 | | Reviewed by Head of Compliance (Next review next academic year.) | 26 February 2025 |
| | | **Date in force** | **27 February 2025** |
| 7.0 | | Reviewed by the Director of Admissions, Compliance and Risk Assurance | 02 February 2026 |
| | | **Date in force** | **09 February 2026** |

The Data Protection and Confidentiality Policy will be reviewed annually by the Document Lead. Any significant changes beyond the scope of an annual review will require the approval of the Board of Directors acting on recommendation from the Senior Management Team (SMT).

# 1. Introduction

This Data Protection and Confidentiality Policy outlines how Bloomsbury Institute handles the Personal Data of its students, staff, Non-Executive Directors, alumni, suppliers, website users and other third parties, in full compliance with relevant data protection legislation.

Any affiliated companies operating outside the UK may be subject to additional rules and regulations relevant to the legal framework of the country in which they operate.

# 2. Legal Framework

The Data Protection Act 2018[1] ('DPA 2018') sets out the framework for data protection law in the UK.

The UK General Data Protection Regulation[2] ('UK GDPR') is a UK law which came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK.

The Information Commissioner's Office (ICO)[3] is the UK's independent body set up to uphold information rights. It offers advice and guidance, promotes good practice, considers complaints, 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**[4].

Included within Appendix A is a set of definitions for key terminology in relation to data protection. Included within Appendix B and Appendix C are the lawful bases for processing any personal data and special categories of personal data.

# 3. Scope

This policy applies to all personal data we process about individuals ('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 e.g. student recruitment agents.

# 4. Roles and responsibilities

The **Data Protection Officer** (DPO) has overall responsibility for data protection compliance. The DPO has those responsibilities laid out in Article 39 of the UK General Data Protection Regulation (UK GDPR). The DPO can be reached at dpo@bil.ac.uk.

All **Heads of Divisions/Departments** are responsible for ensuring that Personal Data in their area is processed in accordance with this Policy and any associated regulations, policies, and procedures and that staff within their area have completed mandatory data protection training. Heads of Divisions/Departments are responsible for ensuring that staff within their area of responsibility apply appropriate practices, processes, controls to comply with this policy.

**All 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.

**Students** must ensure that they are familiar with the Privacy Notice[5] provided by us and ensure that any information they provide to Bloomsbury Institute is kept up to date.

---

[1] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[2] https://www.legislation.gov.uk/eur/2016/679/contents

[3] https://ico.org.uk/

[4] Further details of the Data Protection register entry can be found at https://ico.org.uk/ESDWebPages/Search

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

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.

# 5. 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.

In line with the Data Protection Principles, Bloomsbury Institute will ensure that personal data is:

1. **Processed lawfully, fairly and in a transparent manner in relation to the data subject.**

Bloomsbury Institute's Privacy Notice[6] sets out clearly and publicly how the Institute collects, uses and shares prospective, current and former student's data, and for what purpose. The same Notice seeks to help students understand their rights in relation to the personal data the Institute holds. This ensures that students can make an informed decision about whether or not to provide the data requested.

Personal data relating to staff is processed primarily on the basis of contractual necessity, legal obligation, and legitimate interests, rather than consent. Detailed coverage of data protection matters is provided in individual staff contracts.

All 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.

2. **Collected only for specified, explicit and legitimate purposes.**

Bloomsbury Institute only processes personal data for the specific purposes explained to the data subject at the point of collection. Should the Institute need to use the data for a different and unrelated purpose, the data subject will be informed before any processing takes place. In some cases, consent of the data subject may be required.

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, consent of the data subject is not required.

3. **Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.**

Bloomsbury Institute seeks to collect or process only the minimum amount of personal data required 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.

4. **Accurate and, where necessary, kept up to date.**

The accuracy of any personal data is verified at both the point of collection and at regular intervals afterwards in accordance with our Records Management Policy[7].

Inaccuracies are corrected or erased, as appropriate; however, information will not be deleted if it has been used to inform decisions affecting a data subject. In such cases, the information will be corrected for future use (to ensure it is up to date) and an explanatory note will be added.

Quality of data is verified before transmission – Bloomsbury Institute will not transmit any data that is inaccurate, incomplete or no longer up to date.

5. **Not kept in a form which permits identification of data subjects for longer than is**

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

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

**necessary for the purposes for which the data is processed.**

Bloomsbury Institute will destroy (securely) or erase data from our systems when there is no longer a legal, business or operational requirement for it to be retained, taking into account the purposes for which it was originally requested it. Our Data Protection Officer can advise on periodic reviews based on the retention schedule, which can be found in the Records Management Policy[8].

6. **Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.**

It is of the utmost importance that data is kept securely. Electronic data is hosted on a secure network, and on the secure servers of third-party cloud storage providers with whom we have contractual agreements. All systems are subject to regular vulnerability scans, and security patches must be up to date for IT systems which are being designed and delivered by third-party suppliers prior to becoming operational, as set out in our System Management Policy.

Our Information Security Policy supports compliance by 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.

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 UK, including the use of websites or applications hosted on servers based outside of the UK, unless appropriate safeguards are in place. Appropriate safeguards may include UK adequacy decisions, the International Data Transfer Agreement (IDTA), or other mechanisms approved by the ICO.

Bloomsbury Institute will maintain appropriate records to demonstrate compliance with these principles.

# 6. Data protection by design and default

Bloomsbury Institute is committed to the principle of data protection by design and default. Privacy and data protection issues are fully considered during system, service, product, or process design and development.

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.

All staff must use the minimum amount of data necessary for the purpose and consider the use of anonymised data or pseudonymised data, as appropriate.

A Data Protection Impact Assessment (DPIA) will be conducted where processing is likely to result in a high risk to individuals' rights and freedoms.

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

# 7. Data subject rights

Bloomsbury Institute maintains procedures to enable individuals to exercise their rights under data protection legislation. These rights are set out below.

### 1. The right to be informed

Individuals have the right to clear and concise information about what will be done with their personal data. The Privacy Notice[9] publicly available on Bloomsbury Institute's website explains how the Institute collects, uses and shares personal data, and an individual's rights in relation to the personal data held.

### 2. The right to subject access

Individuals have the right to request to see or receive copies of any information held 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, the Institute reserves the right 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.

### 3. The right to rectification

If personal data is inaccurate, data subjects have the right to require the Institute 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.

### 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 must demonstrate grounds for objecting to the processing, except in the case of direct marketing where it is an absolute right.

### 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 to:

- exercise the right of freedom of expression and information

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

- comply with a legal obligation
- perform a task carried out in the public interest or in the exercise of official authority
- archive 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
- establish, exercise or defend legal claims

**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 by the subject, or data captured on the subject's use of a service, for example, use of online services like our VLE. If technically possible, the Institute will consider transferring information directly to another organisation.

**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 the Institute may 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 the Institute is verifying it
- the data has been unlawfully processed
- the personal data is no longer needed but the individual needs it retained in order to establish, exercise or defend a legal claim
- the individual has objected to the processing their data, and the Institute is considering whether any legitimate grounds override this

**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.

# 8. Record-keeping and statistics

We record key information (for example name, course, contact details, and other biographical information) for administrative purposes. This information may be held on paper and/or electronically.

During meetings with our staff, applicants or students may provide information of a personal and sensitive nature (e.g. concerning their finances, disability, health and wellbeing, family circumstances or other difficulties). A record of the discussion may be kept by us to ensure that the appropriate advice or response is provided, particularly at any subsequent visit. Sometimes additional

correspondence or copies of documents which an applicant or student provides may be attached to these notes.

If the applicant or student is using a service that regularly keeps notes, they will be informed at the start of their consultation. In some cases, in order to ensure that the applicant or student's concerns or issues can be dealt with, it may be necessary for staff to discuss their case with and pass information on to other colleagues within the Institute, academic partners, or to other relevant third parties. The applicant or student will be asked to agree in writing to any notes being kept and to information being passed on.

Academic records containing profiles of module and programme results including coursework, work experience and practice outcomes will be shared among relevant academic and administrative staff and awarding body for the purpose of approval of marks, student progression, and awards.

Final award decisions are considered to be in the public domain. Such awards are published within the graduation awards book. Students may, however, opt for confidentiality and request (via the Data Protection Officer) that their final award outcomes are not published in any form at any time.

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.

The Institute will conduct periodic audits to assess compliance with this Policy, the Data Protection Act 2018 and UK GDPR.

# 9. Confidentiality

With regards to electronic and manual records and the provision of advice and counselling, all applicants, students and staff have a right to expect that information received and recorded by Bloomsbury Institute is treated in absolute confidence, with sensitivity, care and discretion. Personal data will 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:

- Regulatory agencies/bodies such as the Office for Students (OfS) and the UK Visas and Immigration (UKVI)

- Collaborating partners of the institute, such as our awarding body
- Student recruitment agents
- Student Funding Companies
- Friends or family members
- Local authorities
- Government bodies
- The Police

Information is only used for the purposes for which it was provided, and staff will not pass on personal information about applicants or students to anyone outside Bloomsbury Institute (this includes relatives or friends of applicants or students, or external agencies) without the applicant's or student's express written permission, subject to the following exceptions:

- Where there is a legal obligation, for example to release information to the Police, a court of law, Student Funding Companies, the UK Visas and Immigration (UKVI) or other law enforcement agencies. A written request made under the Data Protection Act 2018 will normally be required before this information is released.
- If the applicant or student is under 18 years of age and Bloomsbury Institute has serious concerns about their welfare.
- If Bloomsbury Institute has significant concerns that the applicant or student presents a risk of harm to self or to others.
- For statistical data, for example data that cannot be used to identify any individuals, this could be shared anonymously across the Institute to help spot trends and plan services.

## 10. Disposing of personal data

It is necessary 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.

## 11. Liaison and correspondence

In order for staff to respond effectively to an applicant or student's enquiry or concerns, or the concerns of staff members regarding an applicant or student, it may be appropriate to contact a third party on the applicant or student's behalf. In cases where this is considered to be necessary, the applicant or student's written permission will be sought. If they do not give written permission, other than in the exceptional circumstances outlined in **Section 9** above, staff will not initiate discussion or correspondence with others in any way that allows the applicant or student to be identified. If the

applicant or student does give permission, the nature of the contact will be agreed with them in advance.

In the event that staff receive a request for information about an applicant or student from a third party, including friends and relatives, they will not provide such information without the applicant or student's permission except in cases of genuine emergency or in the exceptional circumstances outlined in **Section 9** above. In such cases, the nature and degree of information to be provided will be agreed in advance with the Data Protection Officer. If staff are unsure to whom they can legitimately disclose personal data, they should seek advice from the Data Protection Officer at dpo@bil.ac.uk.

## 12. Students with a disability, long-term medical condition, or specific learning difficulty

If a student has declared a disability, long-term medical condition or specific learning difficulty, we are legally required under the UK's Equality Act 2010 to make appropriate and reasonable adjustments in order to help students to participate to the fullest extent possible in the educational opportunities provided by Bloomsbury Institute. Information requested from a student about their disability, medical condition or specific learning difficulty will be limited to that which is necessary to ensure that appropriate adjustments can be made to help the student gain maximum benefit from their study.

Any information will normally only be passed to relevant third parties with the student's agreement. Prior to disclosure of any information to a relevant third party the student will be asked to sign a consent form to share their information. If the student does not give permission, this may seriously limit the scope and nature of any adjustments that Bloomsbury Institute can make on behalf of the student.

For further information, contact the Disability and Wellbeing Office[10] for a copy of the Disability Office – What we do with your data

## 13. 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.
- personal data that it will process.
- categories of data subjects to which personal data relates.
- 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.

## 14. Vendors, contractors, and suppliers

Vendors, contractors and suppliers are sometimes 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.

[10] disability@bil.ac.uk

- Required to sign nondisclosure agreements where access to personal data is unavoidable.

# 15. Data breach management

Bloomsbury Institute is responsible for ensuring that staff receive appropriate training; 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[12] could have severe implications for Bloomsbury Institute, and its students and staff and is required to be reported immediately (within 24 hours) to the Data Protection Officer.

The General Data Protection Regulation (GDPR) creates a legal obligation to report certain data protection breaches to the Information Commissioner's Office within 72 hours of identification. Bloomsbury Institute's **Data Breach Management Procedures** set out how we comply with this requirement and how we log, investigate and respond to all reported incidents.

Any breach of data protection law due to unauthorised access, misuse or loss by staff may result in disciplinary action, under Bloomsbury Institute's Staff Disciplinary Procedure[13].

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.

# 16. 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. Concerns or complaints about the Institute's handling of personal data should be directed to the 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[14].

# 17. 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.

# 18. Related regulations, policies and procedures

**External**

- Data Protection Act 2018

[12] 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.

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

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

- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998

**Internal**

- Data Breach Management Procedures
- Information Control Procedures
- Information Security and Management Policy
- Privacy Notice
- Records Management Policy
- Staff Disciplinary Procedure
- Student Complaints Policy and Procedures

## 19. Review of Data Protection and Confidentiality Policy

The Data Protection and Confidentiality Policy will be reviewed regularly by our Senior Management Team (SMT) in line with our Policy Review Schedule. A review may also be triggered because of changes in the legislative requirements. Any amendments require the approval of our Board of Directors.

# Appendix A: Definitions

1. **Personal Data**

   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 (see below). These are considered to be more sensitive and may only be processed in more limited circumstances.

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 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 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. Bloomsbury Institute is the Data Controller.

4. **Data Processor**

   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)**

   The person appointed as such under the UK GDPR and 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**

   An identifiable living person who can be identified, directly or indirectly from personal data. This may include current, prospective and former staff or students, suppliers of goods and services, business associates, etc.

7. **Processing**

   Anything that is done with personal data, including collection, storage, use, disclosure, and deletion.

8. **Special category personal data**

   Sensitive data that requires extra protection. Special category personal data relates to an individual's race, ethnicity, political opinion, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

# 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 interest 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.