The University of Birmingham Data Protection Policy

A. Introduction

During the course of our activities, the University collects and uses data about a wide range of individuals, for example staff, students, applicants, visitors and people taking part in our research. Maintaining the security and privacy of their personal data is essential. Data Protection Law regulates how Personal Data must be processed to protect privacy and provides individuals with rights in relation to their Personal Data. This policy has been reviewed in light of the new Data Protection Act 2018 and the implementation of the EU General Data Protection Regulations 2016 ('GDPR').

The University has policies in place, including this Policy, which are designed to protect the accuracy, integrity, and confidentiality of Personal Data and to ensure that individuals are able to exercise their rights. Appendix 1 provides more information about these other policies.
All Data Users must comply with this Policy when processing Personal Data on behalf of the University.

Key words are defined in the Glossary of Terms in Appendix 2.

B. About the Policy

This Policy has been approved by the University's Executive Board. It sets out the University's requirements as Data Controller when processing Personal Data.

It applies to all types of Personal Data, including Special Category Data. We process data about current, past, and prospective students and members of staff and their family members, people who take part in our research, contractors and suppliers, donors and supporters of the University, customers and clients of services and facilities provided by the University and visitors to the University.

The Policy applies to all Personal Data processed by the University (which

includes any activity involving Personal Data, such as collecting, analysing, sharing, transferring storing, or deleting it) in any media or format. This includes electronic Personal Data, photographic, video or audio Personal Data, Personal Data in the form of human tissue samples, biometric or genomic data and paper records. It also applies whether we collect the information from individuals, whether it is provided to us by those individuals or other people or whether it is collected from other sources.

All staff, students, honorary and associate members of staff and any other University of Birmingham Data Users must comply with this Policy, and disciplinary action can be taken against those who do not comply, particularly in cases when there has been deliberate, wilful or negligent disregard of the Policy and University requirements.

This Policy has the status of a Code of Practice in accordance with University Regulation Section 9 (opens in a new tab).

The University has appointed a Data Protection Officer to advise the University on data protection law, monitor compliance, provide advice to Data Users, and ensure that guidance, training, and resources are available to Data Users. The Data Protection Officer is the point of contact for individuals wishing to exercise their rights in relation to their data, and for any contact with the Information Commissioner's Office. Contact details for the Data Protection Officer and the Information Compliance Manager who deals with general queries and Subject Access Requests are set out in Appendix 3, which also details other sources of information about data protection.

C. Training

Whilst it is recognised that some staff will receive elements of Data Protection training as part of their research requirements, all staff must complete the University's Baseline Data Protection Training, which is available on Canvas. Most staff will be required to complete the module every two years, but some staff may be required to complete it annually because of the nature of their work (e.g., if they work with NHS patient data). New members of staff must complete

this module as part of their induction. It is the responsibility of managers to identify which additional Data Protection Training modules (e.g., for researchers) should be completed by their staff biennially and/or as part of their induction. Manager will receive notification of those staff who are yet to complete the training from the academic year 2018/19, so that they can ensure the training is completed.

It is the responsibility of each Programme Lead and for each supervisor of Postgraduate Research Students to decide whether students must complete the University's Baseline Data Protection Training, or any additional Data Protection Training modules identified as appropriate, at the outset of their programme or annually, and for ensuring completion. More generally the module can be made available to those students undertaking research which involves the use of Personal Data, as required.

D. Data Protection Principles

When processing any personal data, there are 6 data protection principles which the University must follow:

1. Lawfulness and fairness
2. Purpose Limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Security

Further information on the 6 Data Protection Principles can be found in Appendix 4.

The GDPR imposes further restrictions on the transfer of Personal Data outside the European Union, to third countries or international organisations to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

The University has practical resources, advice, and guidance to explain these

principles and how to apply them in practice. More information about where to find these is set out in Appendix 3.

E. Lawful basis for processing

In addition, whenever the University processes Personal data there must be a valid lawful basis for that processing. There are 6 potentially applicable lawful bases for general processing of Personal data and 10 lawful bases for processing Special Category Data. If Special Category Data is being processed, both a lawful basis for general processing and an additional condition for processing this type of data must be identified. These are listed in full in Appendix 5.

The University has practical resources, advice, and guidance to help explain the bases for processing and how to apply them in practice, and more information about where to find these is set out in Appendix 3.

In practice, for many of the University's activities it will rely on the legal basis that the 'processing is necessary for the performance of a task carried out in the public
interest' as this covers our work as a university in teaching and research. However sometimes the University will need to rely on alternative bases.

Particular issues relating to the legal basis for processing Personal Data include:

'Legitimate Interests'

The University can only rely on the 'legitimate interests' basis for processing Personal Data when the University is NOT performing a task carried out in the public interest. Appendix 6 sets out in Part A those activities which the University has determined are University tasks and activities which are carried out in the public interest (or in the exercise of official authority vested in it) and therefore are not classified as being in the University's 'legitimate interests' but rather as 'public tasks'. Appendix 6 Part B sets out those activities which it has determined are not part of the University's "public tasks" but which may be

within its ‘legitimate interests’. The Data Protection Officer must be notified before processing any Personal Data on the basis of the legitimate interests of the University or a third party in relation to an activity which is not listed in Part B of Appendix 6, to confirm that ‘legitimate interest’ is the correct legal basis for processing.

Criminal Offence Data

The requirements for processing Criminal Offence Data have been clarified under the GDPR and the Data Protection Act 2018. These are set out in Appendix 7.

The University’s Executive Board may approve additional policies from time to time relating to the processing of Criminal Offence Data in line with the principles set out in this Policy.

‘Substantial public interest’ condition

When processing Special Category Data in reliance on the ‘substantial public interest’ basis, the requirements set out in Appendix 8 must be followed. The University’s Executive Board may approve additional policies from time to time relating to the processing of Special Category Data on the basis of ‘substantial public interest’ in line with the principles set out in this Policy.

Profiling and Automated Decision Making

When processing Personal Data by Profiling or Automated Decision Making, the requirements set out in Appendix 9 must be followed.

F. Individuals Rights

In accordance with the GDPR and the Data Protection Act 2018 every Data Subject has the following rights:

1. The right to be informed about how their Personal Data is to be used.
2. The right of access to their Personal Data held by the University and other information.
3. The right to rectification if their Personal Data is inaccurate or incomplete.
4. The right to request the deletion or removal of Personal Data where there

is no compelling reason for its continued processing.

5. The right to restrict processing in certain circumstances.
6. The right to data portability which allows individuals to obtain and reuse their Personal Data for their own purposes across different services.
7. The right to object to processing in certain circumstances.
8. Rights in relation to automated decision making and profiling.

More information for Data Subjects (opens in a new tab) wishing to exercise these rights can be found on the University's website, and in particular information about Subject Access requests (opens in a new tab).

The University must respond to any requests from Data Subjects wishing to exercise these rights within strict time limits. Therefore, all requests from individuals wishing to exercise rights must be forwarded to the Data Protection Officer immediately.

Similarly, staff must prioritise requests from the Data Protection Officer to assist with processing a Data Subject request, to ensure compliance with Data Protection Laws.

G. Queries, Concerns and Complaints

Any queries or concerns about the processing of Personal Data by or on behalf of the University or in relation to the exercise of any Data Subject rights should contact the Information Compliance Officer in the first instance.

Complaints about the processing of Personal Data should be made to the Data Protection Officer.

Any person who is not satisfied with the way the University has handled Personal Data or a request to exercise Data Subject rights may complain to the ICO.

Contact details are set out in Appendix 3.

H. Personal Data Breaches

It is important that that Personal Data Breaches are identified and reported to the Data Protection Officer as soon as possible. Some types of Personal Data Breach must be reported to the Information Commissioner's Office by the University's Data Protection Officer within 72 hours. Staff and students must therefore report Personal Data Breaches or potential breaches as soon as possible, as the sooner action is taken, the greater the opportunity to limit any potential damage which might be caused by the incident. The Data Protection Officer will decide whether it is necessary to report the Personal Data Breach to either the Information Commissioner's Office for the affected Data Subjects, or necessary third parties.

Changes to this Policy

This Policy was approved by the University's Executive Board on 16 July 2018. The University may change this Policy at any time, and where appropriate, we will notify Data Subjects of those changes.

Appendices:

Appendix 1: University Policies

Data Management Policy (opens in a new tab)

Information Security Policy (opens in a new tab)

General Conditions of Use of Computer and Network Facilities (opens in a new tab)

Other IT policies, standards, guidance and procedures (opens in a new tab)

Code of Practice for Research (opens in a new tab)

Appendix 2: Glossary of Terms

Term	Description
Automated Decision-Making	Automated decision making is a decision made by automated means without any human involvement.
Baseline Data Protection Training	30-minute training module available to all staff through Canvas Virtual learning Environment
Criminal Offence Data	Data relating to criminal convictions and offences or related security measures.
Data Controller	An organisation which determines the purposes and means of processing Personal Data.
Data Processor	An organisation or person which is responsible for processing personal data on behalf of a Data Controller.
Data Protection Laws	Any law which relates to the protection of individuals with regards to the processing of Personal Data including Regulation (EU) 2016/679 (known as the General Data Protection Regulation or GDPR), the Data Protection Act 2018 and all legislation enacted in the UK in respect of the protection of personal data, and any code of practice or guidance published by the Information Commissioner's Office.
Data Retention Principles	Data retention principles are set out in the University's privacy notices (opens in a new tab)
Data Subject	An identifiable person who can be identified, directly or indirectly from Personal Data.
Data Users	Staff, students, and others who have access to and use Personal Data on behalf of the University.
Personal Data	Any data or information or any combination of data relating to an identifiable person who can be

	directly or indirectly identified in particular by reference to an identifier. These identifiers can include a name, an 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 person.
Personal Data Breach	The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data, including those that are the result of both accidental and deliberate causes.
Profiling	Any form of automated processing of Personal Data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Special Category Data	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Appendix 3: Sources of Information and Guidance

Data Protection Officer

Dr Nicola Cárdenas Blanco, Director of Legal Services, The University of Birmingham, Edgbaston, Birmingham, B15 2TT

Tel: 0121 414 3916

Email: legalservices@contacts.bham.ac.uk

General Queries and Data Subject Requests

The Information Compliance Manager, The University of Birmingham, Edgbaston, Birmingham, B15 2TT

Tel: 0121 414 3916

General queries email: legalservices@bham.ac.uk

Subject Access Requests email: dataprotection@contacts.bham.ac.uk

Data Protection Resources

ICO resources (opens in a new tab)

University resources - Legal Services intranet site (opens in a new tab)

Canvas - Data Protection (GDPR) training module (opens in a new tab)

Personal Data Breach Reporting

Guidance and reporting form (opens in a new tab)

University Information Security Resources

IT Security information and contact details (opens in a new tab)

IT policies, standards, and guidance (opens in a new tab)

IT Security online training (opens in a new tab)

Information Commissioner's Office

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745

Appendix 4: Data Protection Principles

1. Lawfulness and fairness

Personal Data should be processed lawfully, fairly and in a transparent manner.

For data to be processed transparently, individuals must be given clear and adequate information before their Personal Data is collected to enable them to understand how and why their Personal Data is to be used so they can take an informed decision about whether to provide the data. This is often done using a Privacy Notice. The University has prepared separate privacy notices for the different categories of people the University processes information about, for example, students, staff, alumni, visitors, etc, which are on the University website (opens in a new tab).

For data to be processed lawfully, one of the legal bases set out in Data Protection Law must also apply – see below.

2. Purpose Limitation

Personal Data should be collected for specified, explicit and legitimate purposes.

It should not be further used or re-used for new or different purposes (unless one of the exceptions in Data Protection Law applies).

3. Data minimisation

Personal Data processed should be adequate, relevant, and limited to what is necessary in relation to the specified purposes for which they are processed.

Whenever possible, Personal Data should be anonymised or pseudonymised at the earliest opportunity.

4. Accuracy

Personal Data processed should be accurate and, where necessary, kept up to date.

5. Storage limitation

Personal Data should be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the Personal Data are processed.

When no longer needed for the purpose for which it was collected, and if there is no lawful basis for continuing to keep it, the Personal Data must be either fully anonymised or deleted in accordance with the University's high level Data Retention Principles and any relevant departmental data retention schedule.

6. Security

Personal Data should be 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.

Appendix 5: Legal bases for processing

6 legal bases for general processing of Personal Data

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.

b) Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

c) Processing is necessary for **compliance with a legal obligation** to which the data controller is subject.

d) Processing is necessary in order to **protect the vital interests** of the data subject or of another natural person.

e) Processing is necessary for the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the data controller.

f) Processing is necessary for the purposes of the **legitimate interests** pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (This does not apply to processing carried out by public authorities, such as Universities, in the performance of their public tasks).

10 legal bases for processing Special Category Personal Data

a) The data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes.

b) Processing is necessary for the purposes of carrying out the obligations and rights of the data controller or of the data subject in the field of **employment and social security** (subject to the Data Protection Act 2018).

c) Processing is necessary to protect **the vital interests of the data subject** or of another natural person where the data subject is physically or legally incapable of giving consent.

d) Processing is carried out in the course of its legitimate activities with appropriate

safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim** and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

e) Processing relates to personal data which are **manifestly made public by the data subject**.

f) Processing is necessary for the establishment, exercise or **defence of legal claims** or whenever courts are acting in their judicial capacity.

g) Processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

h) Processing is necessary for the purposes of **preventive or occupational medicine**, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to safeguards.

i) Processing is necessary for reasons of public interest in the area of **public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; L 119/38 EN Official Journal of the European Union 4.5.2016.

j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, respect the essence of the right to data protection and provide suitable and specific measure to safeguard the fundamental rights and the interests of the data subject.

Appendix 6: Tasks which are and which are not performed in the public interest or in the exercise of official authority vested in the University

Note: The lists below are not exhaustive. Decisions on whether a particular activity or task is carried out in the public interest or in the exercise of official authority vested in the University must be taken in consultation with the Data Protection Officer or her nominee

Part A: Tasks which are performed in the public interest or in the exercise of official authority vested in the University:

- Teaching
- Research
- The conferral of awards
- Museums, galleries, cultural collections

Part B: Tasks which are not performed in the public interest or in the exercise of official authority vested in the University, but which may use the legal basis for processing as within the University's 'legitimate interests':

- Fundraising
- Alumni relations
- Provision of hotel and conference facilities
- Events hosted on University premises which are not organised by or on behalf of the University
- Services and facilities provided for the business community, third party organisations and members of the public

Appendix 7: Specific issues relating to processing Criminal Offence Data

This Appendix sets out the University's requirements in relation to the processing of Criminal Offence Data for the following purposes.

Processing of Criminal Offence Data to which this Policy Applies

This will include, but is not limited to, the following processing of Personal Data:

a. Criminal Offence Data including DBS checks relating to staff and workers in connection with their employment or work or application for employment or work with the University if it is appropriate, given the nature of the role, and when it is authorised by law and in particular the Rehabilitation of Offenders Act 1974 as amended. This is processed to comply with employment and other laws, to consider suitability for employment or continued employment or to consider safeguarding issues.

b. Criminal Offence Data relating to and disclosed by individuals who apply to the University for a place on a programme of study which requires a satisfactory Disclosure & Barring Service (DBS) check to be carried out before the individual can be accepted on to, or continue with, a programme of study or in connection with a module or other component comprising part of a programme of study. This is necessary to protect the interests of patients, clients, children, and vulnerable people.

c. Criminal Offence Data relating to and disclosed by individuals who apply to the University for a place on any other programme of study*.

d. Criminal Offence Data relating to Registered Students who are convicted of a criminal offence between the date on which they are offered a place on a programme of study and the date on which they leave the University*.

*Criminal Offence Data referred to in c. and d. above is processed in order to assess and, if necessary, manage appropriately and proportionately any risks to the Data Subject, other students, staff, service users or others with whom the Data Subject will have contact as a member of the University. This is under

review and the Policy may be revised to reflect any agreed changes.

e. Criminal Offence Data in relation to participants in research conducted in the public interest by the University.

f. Criminal Offence Data in relation to volunteers working on behalf of the University in regulated activity with children and adults.

Requirements

Before collecting and processing Criminal Offence Data:

- a Data Protection Impact Assessment must be carried out by the relevant School or Professional Service and approved by the Data Protection Officer (or nominee). This must be retained and regularly reviewed and revised as necessary for the duration of the processing;
- appropriate measures, including technical and organisational measures, are implemented to ensure appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. These must be regularly reviewed and revised as necessary for the duration of the processing, and records of those reviews must be retained
- staff who will have access to this data must have completed appropriate data protection training before processing the data;
- a clear and transparent Privacy Notice has been provided to Data Subjects which includes a specific indication of how long the Personal Data will be retained for and when it is likely to be erased. The Data Protection Officer (or nominee) must be consulted in relation to the Privacy Notice; and
- a record is maintained which must include the following information:
  a) The relevant condition for processing in the Data Protection Act 2018 which is relied on.
  b) The legal basis for processing.
  c) Whether the data is retained and erased in accordance with the applicable Retention Principles and the information set out in the relevant Privacy Notice relating to retention and erasure and, if it is not, the reasons for not

following those policies.

Advice on compliance with these requirements can be obtained from Legal Services.

Appendix 8: Policy for Processing Special Category Data based on the 'Substantial Public Interest' condition for processing

Before processing Personal Data when relying on the 'substantial public interest' condition for processing:

- a Data Protection Impact Assessment must be carried out and approved by the Data Protection Officer (or nominee). This must be retained and regularly reviewed and revised as necessary for the duration of the processing;
- appropriate measures, including technical and organisational measures, must be implemented to ensure appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. These must be regularly reviewed and revised as necessary for the duration of the processing, and records of those reviews must be retained.
- those who are to have access to this data must have completed appropriate data protection training before processing the data;
- a clear and transparent Privacy Notice has been provided to Data Subjects which includes a clear indication of how long the Personal Data will be retained and when it is likely to be erased. The Data Protection Officer (or nominee) must be consulted in relation to the Privacy Notice; and
- a record is maintained which must include the following information:
  (a) The relevant condition in the Data Protection Act 2018 which is relied on.
  (b) The legal basis for processing.
  (c) Whether the data is retained and erased in accordance with the applicable Retention Principles and the information set out in the relevant Privacy Notice relating to retention and erasure and, if it is not, the reasons for not following those policies.

Appendix 9: Policy in relation to Profiling and Automated Decision Making

The ICO has produced guidance on Profiling and Automated Decision Making (opens in a new tab) which is available on its website which should be considered before considering any activity or task which involves Profiling or Automated Decision Making.

Before starting a task or activity which involves Profiling or Automated Decision Making, the following steps must be carried out:

1. A Data Protection Impact Assessment (DPIA) must be carried out. The Data Protection Officer must be informed and consulted as part of that exercise.
2. A Privacy Notice must inform individuals if their data will be used for solely automated decision-making processes with legal or similarly significant effects. This must explicitly set out the Data Subject's rights. The Privacy Notice should be approved by the Data Protection Officer.
3. The DPIA must be kept under regular review, and records of those reviews must be retained.