Version	2.4
Reviewed Date	15/06/2023

Data Protection and Privacy Policy

1. Introduction

1.1 General

The University holds and processes information about employees, students, and other data subjects for academic, administrative and commercial purposes. the University, and all staff or others who process or use any personal information, must comply with the Principles which are set out in Data Protection law when handling such information,

In summary these state that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner (‘lawfulness, fairness and transparency’)
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
4. Accurate and, where necessary, kept up to date (“accuracy”)
5. Kept in a form which permits identification for no longer than is necessary for the purposes for which the personal data are processed (“storage limitation”)
6. Processed in a manner that ensures appropriate security using appropriate technical or organisational measures of the personal data (“integrity and confidentiality - security”)
7. The controller shall be responsible for and be able to demonstrate compliance with the principles (“accountability”)

1.2 Definitions

“**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 identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**Staff**", "**students**" and "**other data subjects**" may include past, present and potential members of those groups.

"**Other data subjects**" and "**third parties**" may include contractors, suppliers, contacts, referees, friends or family members.

"**Processing**" refers to any action involving personal information, this includes emailing collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Data Subjects" refers to any natural person whose personal data the University processes or is likely to process.

"Data Protection Law" in the UK principally refers to the 2018 Data Protection Act ('the Act' and the UK GDPR) as well as common law.

"Special Category Data" is personal data which the Act defines specifically and which requires additional legal safeguards. Types of personal data which fall into special categories are defined in 7.1

2 Privacy Notices

2.1 Standard Privacy Notices

The university will provide a privacy notice at the point of collection of personal data in order to provide fair and transparent processing under the first principle

This will contain:

- Purpose of Processing
- Legal basis and reason for Processing
- With whom personal data will be shared
- Information about international transfers
- A list of subjects' rights
- Consequences of not providing the data
- Details of any automated processing
- Retention periods
- Contact details of the Brookes' Data Protection Officer
- Contact details of the Regulator (Information Commissioner)

Where the data has not been acquired directly, the University will state:

- What types of personal data we will use and why
- The source of the personal data

2.2 Summary Privacy Notices

In some instances, it will be impractical or impossible to display a full privacy notice. In such cases we will display a summary privacy notice which will contain:

- Data protection contact details for the University
- Purpose of the processing

- Legal basis for processing
- Link to the full privacy notice

3. Staff Responsibilities

3.1 Staff Personal Data

All staff are data subjects of the University and are subject to the rights listed in section 5.2

3.1.1 Data protection compliance is the responsibility of the entire university and staff must ensure that personal data the university holds on them is kept accurate and up to date.

3.2 Processing Personal Data

3.2.1 Staff shall ensure that appropriate organisational and technical measures are taken to secure any personal data that is processed. This includes:
Personal data is stored securely and access to personal data is controlled on a need to know basis
All reasonable steps are undertaken to ensure that personal data is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party. Unauthorised disclosure may be a disciplinary matter for staff and may be considered gross misconduct in some cases. Any such incidents must be reported to the IT Information Security Team in accordance with the requirements of the Information Security Incident Management Policy

- Staff are required to adhere to IT Acceptable Use Policy (see here)

3.2.2 All staff must undertake the University's mandatory Information Security Awareness Training every two years or as prescribed

4. Student Responsibilities

4.1 All students shall ensure that all personal information which they provide to the University is accurate and up-to-date; and

4.1 .1 Inform the University of any changes to that information.

4.12 Students should check periodically that any personal data the University holds about them and either update it through a self-service portal or inform the University of any amendments or corrections which are needed.

4.2 Students who use the University IT facilities may, from time to time, process personal information (for example, in course work or research). In those circumstances, they must notify their course tutor or research supervisor in the relevant Faculty who will provide further information about their responsibilities in processing personal data.

5. Rights of Data Subjects

5.1 Right of Access

5.1.1 Staff, students and other data subjects of the University have the right to access personal data about them. Any person may exercise this right by submitting a request in writing to the IT Services Information Security Team.

5.1.2 The University will not make a charge for such requests. Where the University deems the requests to be manifestly unfounded or excessive the University will charge a fee based on resources needed to fulfil the request.

5.1.3 The University aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within one month except where requests are complex or numerous. In such cases the statutory time frame can be extended by two months. The reason for any extension will be explained in writing by the Information Compliance Team to the data subject making the request within one month of the initial request being made.

5.2 Other Rights

5.1.1 Data subject may have additional rights under the legislation:

- The right to be informed
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object to the processing of data
- Rights in relation to automated decision making and profiling.

5.1.2 The University will take appropriate steps to ensure necessary policy and procedures are in place to allow subjects to exercise their rights as stated in 5.1.1.

6. Lawful Processing and Consent

6.1 The University must provide a lawful basis for processing any personal data. The University will use the following lawful bases:

- **Consent**: the subject has given clear consent for the University to process their personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract the University has with the individual, or because they have asked the University to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for the University to comply with the law.
- **Vital interests**: the processing is necessary to protect someone's life.

- **Public task**: the processing is necessary for the University to perform a task in the public interest or to carry out official functions, and the task or function has a clear basis in law (core business)

- **Legitimate interests** - Processing is necessary for the purposes of the legitimate interests pursued by the University with full consideration to safeguard the rights and freedoms of the data subject.

7. Special Category Data & Criminal Convictions

7.1 The University will not process any data relating to:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data or biometric data
- Health data
- Sexual life or sexual orientation
- Criminal proceedings or convictions

Unless one of the conditions is 7.2 is fulfilled.

7.2 The University will only process special categories where:

- Explicit consent of the subject has been obtained
- Processing is necessary for employment, social security or social protection purposes
- It is necessary to protect the vital interests of the subject themselves or others
- It is necessary for the legitimate interests of the university and will not be shared externally without consent
- The data has been made public by the data subject
- It is necessary for legal proceedings or is otherwise lawful
- It is necessary for reasons of substantial public interest
- It is necessary for medical or social care reasons
- It is necessary for reasons of public interest in the area of public health
- It is necessary for archiving purposes

8. Data Protection Officer

8.1 Designation of the Data Protection Officer (DPO).

8.1.1 The University has a Data Protection Officer

8.1.2 The University's Information Security Team will be the point of contact and will facilitate appropriate information sharing with the designated DPO.

9. Retention of Data

9.1 The University processes personal data for many different lawful purposes. The University will maintain a records retention schedule on which decisions on how long personal data can be retained for the specified purpose. The retention schedule is published and can be found here.

10. Compliance

10.1 Compliance with the Data Protection and Privacy law is the responsibility of all students and members of staff. Any deliberate or reckless breach of this Policy may lead to disciplinary, and where appropriate, legal proceedings. The University has a dedicated Information Security Team and any questions or concerns about the interpretation or operation of this policy should be taken up with them in the first instance by email at info.sec@brookes.ac.uk. This is a team email address

10.2 Any data subject who considers that the policy has not been followed in respect of their personal data can report it to the University Information Security Team.

11. Data Protection Breach Management

11.1 A data protection breach is where any personal data held by the University, in any format, is compromised by being lost, destroyed, altered, copied, transmitted, stolen, used or accessed unlawfully or by unauthorised individuals whether accidentally or on purpose. Such as:

- Loss or theft of equipment on which data is stored, e.g. laptop or mobile phone
- Unauthorised access to data
- Emails sent to wrong recipients
- Public posting of confidential material online
- Incorrect sharing of Google (or any) documents
- Failure of equipment or power leading to loss of data
- Hacking attack
- Data maliciously obtained by way of social engineering

11.2 The University shall maintain and publish an Information Security Incident Management Policy. This Policy can be found here.

11.3 All such breaches must be reported immediately to The IT Service Desk, or the ServiceNow Portal https://service.brookes.ac.uk/brookes/)

12. Register of Processing Activity

12.1 The University shall maintain a register of processing activity

12.2 The register described in 12.1 shall be periodically updated when required and reviewed by data owners at least once within a period of 12 calendar months.

13. Data Protection Privacy Impact Assessments (DPIA)

13.1 Where there is a new, or change of existing processing activity, which may result in a risk to the rights and freedoms of data subjects (privacy intrusive), the University will conduct a Privacy Impact Assessment (DPIA).

13.2 The University will embed DPIA within its project governance procedures so that privacy risks are identified and assessed at point of proposal.

13.3 Any changes to existing processing activities captured in the register of processing activity deemed to be privacy intrusive will require a PIA.

14. Processing Personal Data for Research

14.1 Where processing data for research purposes you must ensure that you obtain consent in accordance with the Act

14.2 The University Research Ethics Committee (UREC) will be able to provide assistance.

You can find guidance at:
https://www.brookes.ac.uk/sites/research-support/research-ethics-and-integrity/research-ethics

15. International Personal Data Transfers

15.1 The University will only transfer data within the UK and the EU or to a country or international organisation which has a finding of adequacy of protection for the rights and freedoms of the data subjects, save where an acceptable level of risk has been assessed and determined based on the facts of the transfer, or: the data subject has explicitly consented to the proposed transfer

16. Personal Data Processed by Third Parties and Suppliers

16.1 Where the University uses third parties and suppliers (to be known as processors in this section) to process personal data. The University shall:

- Use only processors providing sufficient guarantees to implement appropriate technical and organisational measures to facilitate data security as the law requires.

- Seek assurances that the processor shall not engage another processor without prior specific or general written authorisation of the controller in advance of so doing.

- Processing by a processor shall be governed by a contract in which the processor or otherwise by written or formal agreement:

- Only processes the personal data only on documented instructions from the controller

- Ensures that persons authorised to process the personal data have committed themselves to confidentiality

    - Assists the controller in the fulfilment of requests exercising the data subject's rights.
    - Deletes or returns all the personal data to the controller after the end of the contract.

- Agree to regular audits by the University.

17. Data Protection Audits

17.1 The University will periodically undertake data protection audits. These will include:

- Auditing of internal policies and procedures
- Auditing of planned projects and changes to systems (via privacy impact analysis)
- Auditing of contractual terms
- Auditing of supplier policies and physical security measures.