Data Protection Policy

Responsible Office	Governance, Legal & Compliance
Responsible Officer	University Secretary
Approval authority	Audit Committee
Date of approval	June 2022
Amended (if applicable)	N/A
Related University Policies	Research Data Policy Regulations for the Use of Computer Facilities Privacy Notices
Related Procedures	Data Breach Procedure
Effective Date	June 2022
Supersedes	v. May 2018
Next review due	June 2027

1 Introduction

1.1 Bath Spa University is committed to a policy of protecting the rights and privacy of individuals (including students, staff and others) in accordance with Data Protection Laws. The University commits to:

- Processing personal data fairly and legally by appropriately applying the Data Protection Principles (see section 4);
- Supporting and enabling the rights of individuals under Data Protection Laws;
- Keeping personal data secure by implementing appropriate technical and organisation security measures; using appropriate contracts with third party organisations who may act as data processors on the University's behalf or as separate data controllers; holding relevant records about the personal data we process; and ensuring adequate safeguards are in place whenever personal data is transferred to a third country.
- Designing privacy into our systems and processes and conducting Data Protection Impact Assessments where necessary.
- Cooperating with and being responsive to relevant guidance from the Information Commissioner's Office (ICO).

1.2 The purpose of this policy is to set out a summary of the University's responsibilities under Data Protection Laws and make clear the specific responsibilities for data protection compliance within the University. Key terms used within this policy are defined in **Appendix 1**.

2 Scope

2.1 The University is required to comply with Data Protection Laws and to register as a Data Controller with the Information Commissioner's Office. The University's notification (registration number: Z7222773) covers the University's academic activities, administrative functions, and business operations, including its wholly-owned subsidiary companies. The University is an exempt charity, and a "public authority" according to the definitions set out in the Data Protection Laws.

2.2 The types of personal data that the University may be required to handle include information about current, past and prospective students, employees, officers, governors, suppliers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, are subject to certain legal safeguards specified in Data Protection Laws and associated legislation. The use of this personal data is as laid out in our Privacy Notices. The University recognises that the correct and lawful treatment of this data will maintain confidence in the University and will provide for successful academic and business operations.

2.3 This policy and any other documents referred to in it set out the basis on which the University will process any personal data it collects, or that is provided to the University by data subjects or other sources. It sets out the rules on data protection and the legal conditions that must be satisfied when the University processes personal data.

2.4 This policy applies to, and must be adhered to, by all staff and other authorised University representatives processing data on behalf of the University. The term 'staff' means anyone working in any context within the University at whatever level

or grade and whether permanent, fixed term or temporary, including but not limited to employees, workers, and agency staff. The term "authorised University representatives" means other individuals given authorised access to Personal Data for the purposes of activities they perform for or on behalf of the University where and to the extent that this is specified in the terms of their authorisation, including but not limited to Governors, retired but active research staff, other visiting research or teaching staff, agents, volunteers, contracted service providers and external members of committees.

2.5 This policy also applies to students of the University when processing personal data on behalf of the University whether as part of research activities, group study, performance, experiments, fieldwork and case studies, and to students who are employed by the University. It does not apply to students when acting in a private or non-University capacity.

2.6 This policy does not form part of any employee's contract of employment and should be read and complied with in conjunction with other associated University policies and procedures.

2.7 Third parties who process personal data on behalf of the University also have obligations under Data Protection Laws. See section 9 below for further details.

3 Roles and Responsibilities

3.1 The University has a responsibility to comply with Data Protection Laws.

3.2 The Board of Governors is responsible for overseeing the conduct of the affairs of the University and for safeguarding its assets (including information assets). The Audit Committee of the Board of Governors is responsible for approval and oversight of this Data Protection Policy.

3.3 The University Secretary fulfils the role of Data Protection Officer (DPO). The DPO as required by the Data Protection Laws, is an independent role and is responsible for monitoring and leading University compliance with the Data Protection Laws and with this policy. The DPO can be contacted at data-protection@bathspa.ac.uk and is supported by the University's Information Compliance Manager.

3.4 The Information Governance Group is responsible for establishing and overseeing the programmes of activity required to protect the University's information assets, including with regard to Data Protection law.

3.5 The Information Compliance Manager sits within the Governance, Legal and Compliance Department, and supports the DPO. The Information Compliance Manager is responsible for:

- providing advice, guidance, training and tools relating to the Data Protection Laws and ICO guidance, to help University departments, schools, staff and authorised University representatives comply with this policy and the Data Protection Laws. This includes assisting with the completion of Data Protection Impact Assessments and advising on data sharing and data processing agreements;
- publishing and maintaining core privacy notices and supporting with other relevant University-wide data protection documents, including the retention schedule and the Record of Processing Activities.

- handling data subject rights requests.

- handling personal data breaches, in accordance with the University's Data Breach Procedure.

3.6 Senior Management, Heads of Schools/Departments and line managers are responsible for:

- making all staff and authorised University representatives within their respective areas aware of this policy, and other related, policies and procedures, and their responsibilities under these, including the completion of mandatory training;

- ensuring that all staff and authorised University representatives within their area are engaged with, follow and complete appropriate processes to enable compliance with the Data Protection Laws;

- ensuring that appropriate resources and processes are implemented within their areas to enable the completion and review of the University's Record of Processing Activities.

3.7 All University staff and authorised University representatives have the following responsibilities:

- familiarising themselves with this policy and their responsibilities under it in relation to Data Protection Laws;

- adhering to the data protection principles (see section 4) when processing personal data as part of their work or activities for the University;

- completing relevant data protection training, including (as a minimum for University staff) data protection training upon induction, and data protection refresher training as required;

- following relevant University data protection advice and guidance relevant to their role, regardless of whether access to, and processing of, personal data is through University-owned and managed systems, or through their own or a third party's systems and devices;

- when processing personal data on behalf of the University, only using it as necessary for fulfilling their contractual duties and/or other University roles, in line with the purposes and practices communicated to individuals by the University privacy notices and associated statements during data collection, and not disclosing it unnecessarily or inappropriately;

- recognising, reporting internally via the appropriate procedures, and cooperating with any remedial work arising from personal data breaches;

- cooperating with the University's fulfilment of data subject rights requests;

- advising students who are using personal data in their studies and research of relevant advice, guidance and tools/methods to enable them to handle such personal data in accordance with this policy and other related policies and procedures;

- taking responsibility for implementing data protection by design and default principles, as appropriate, from the start and throughout the lifecycle of any project they are responsible for. This includes, but is not limited to, completing

Data Protection Impact Assessments, updating Records of Processing Activity and ensuring that privacy notices are appropriately updated.

3.8 Students have the following responsibilities:

- familiarising themselves with the Privacy Policy when they register with the University.
- ensuring that the personal data which they provide to the University is accurate and up to date.
- If processing personal data as part of their research or studies, they must consult with their supervisor before any processing takes place and follow all appropriate University policies and procedures.
- If a student is also employed by the University, they will have the responsibilities of all staff as set out above in respect of any processing of personal data carried out in the course of their employment.

4 Data Protection Principles

4.1 The University is required to process personal data in accordance with the following six data protection principles:

- **Lawfulness, fairness and transparency**: the University must explain to staff, students and other third parties, at the point of collection, how their personal data will be used.
- **Purpose limitation**: the University must only use the personal data it holds in accordance with the purpose for which it was collected.
- **Data minimisation**: the University must only collect personal data which is relevant to the purposes for which it is required; the University must also make sure that enough relevant personal data is collected for any specific purpose.
- **Accuracy**: the University must take all reasonable steps to ensure that any personal data held is correct and up to date and be able to rectify any mistakes promptly.
- **Storage limitation**: the University must not keep personal data for longer than is necessary.
- **Appropriate technical and organisational security measures**: This means that the University must take all reasonable steps to protect the personal data it holds against unauthorised access, loss or destruction.

5 Accountability

5.1 The University, as a data controller, is responsible for ensuring that the appropriate technical and organisational measures are put in place to comply with the Data Protection Laws, including:

- adopting and implementing data protection policies and appropriate security measures;
- ensuring that procedures and process reflect data protection requirements, and reviewing these as required;

- ensuring appropriate arrangements are in place with, and appropriate verification has been carried out in respect of organisations that process personal data on the University's behalf;

- maintaining documentation of the University's processing activities;

- recording personal data breaches and reporting breaches to the Information Commissioner's Office when required;

- carrying out Data Protection Impact Assessments for processing activities that are likely to result in a high risk to the interests and rights of data subjects;

- Creating a culture that values and prioritises privacy issues; and

- Ensuring staff are trained in data protection and aware of their responsibilities.

6 Legal Basis for Processing Personal Data

6.1 The University must meet one or more of the following six legal bases in order to be able to process personal data:

- the data subject has given **consent** to the processing for one or more specific purposes. This consent must be provided by way of a positive action and a record of consent must be maintained. It must be as easy for the subject to opt out as it was for them to opt in;

- processing is necessary for the **performance of a contract** or to take steps, at the request of the data subject, prior to entering into a contract; for example, processing carried out by the University in order to provide services to subjects, including staff and students;

- processing is necessary for compliance with a **legal obligation**. There must be a specific piece of legislation which requires the personal data to be processed;

- processing is necessary in order to protect the **vital interests** of an individual. This is mainly relevant in 'life or death' situations only;

- 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 University. The University may be able to rely upon this for any activities carried out under its public function, such as the retention of student transcripts and the management of staff.

- processing is necessary for the purposes of the **legitimate interests** pursued by the University, except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject. This legal basis can only be relied upon for the private functions of the University, such as the management of alumni, charitable works and some marketing functions.

6.2 Due to its sensitive nature, the University must fulfil further conditions, in addition to the above, in any circumstances in which **Special Category Data** is being processed. These conditions are set out in the Data Protection Laws and advice is available from the Information Compliance Manager. Special Category Data is defined as:

- personal data revealing racial or ethnic origin;

- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

6.3 The legal basis for processing (and where applicable, any further conditions for processing) should be determined before the personal data is processed and documented. The University's privacy notices broadly outline the legal bases for processing carried out as part of the University's standard functions.

7 Research Data

7.1 In addition to this policy, the University shall have in place appropriate policies, processes and training to cover the processing of personal data (and other data) in connection with research projects. The Research Support Office should be consulted in the first instance.

8 Data Subject Rights

8.1 Individuals have a number of rights under Data Protection legislation. These rights are:

- **the right to be informed**: the University must provide individuals with clear and concise information detailing how their personal data is used. This is normally done by way of a privacy notice;
- **the right of access**: this is also known as a subject access request and allows individuals to request a copy of any personal data that the University holds about them;
- **the right to rectification**: this allows an individual to request that any inaccurate or out of date information held by the University about them is corrected.
- **the right to erasure**: an individual can, in certain circumstances, request that the University deletes the information that is held about them;
- **the right to restriction of processing**: an individual may, in certain circumstances, request that any processing of their personal data is ceased.
- **right to data portability**: in certain circumstances, an individual can request a re-usable, electronic copy of their data. This can then be transferred to another provider to allow a comparison;
- **right to object**: individuals may object to any processing undertaken by the University if it is based on legitimate interests or a task carried out in the public interest. This right is absolute if the data is being used for direct marketing purposes.

- **rights in relation to automated decision making and profiling**: if the University is making decisions about an individual using automated means, such as a computer algorithm, they are able to appeal this and request human intervention.

8.2 The University shall have appropriate processes in place to enable it to comply with and respond to any request made by a data subject to exercise any of these rights. These processes shall set out the roles and responsibilities of University staff and authorised University representatives as well as the DPO and the Information Compliance Manager in handing such requests.

8.3 The University's process for handling a subject access request shall include how such requests may be made to the University (and how to recognise these), that in most circumstances the University will not charge a fee to respond to the request, the timescales for response, and how the response will be shared. The process will also set out the circumstances in which the University may refuse to respond to a subject access request.

9 Sharing Personal Data

9.1 The University shall have in place appropriate processes and documentation to ensure that the sharing of personal data with third parties (such as other data controllers and / or data processors) complies with Data Protection Laws and guidance issued by the Information Commissioner's Office.

9.2 In respect of international transfers, personal data must not be transferred outside of the United Kingdom unless appropriate safeguards are in place to ensure an equivalent level of data protection. Generally, such safeguards will be limited to the following:

- **adequacy decision**: the United Kingdom has made a decision that the third country to which the personal data is transferred ensures an adequate level of protection; or

- **UK approved standard contractual clauses and/or addendum to EU approved standard contractual clauses**: specific contractual clauses, adopted by the UK Government, are in place which provide appropriate safeguards of personal data and enforceable rights for data subjects.

10 Data Protection by Design and Default

10.1 The University is committed to ensuring that management and mitigation of privacy risks are built into its operations and projects. Under Data Protection Laws, organisations are required to complete a Data Protection Impact Assessment (DPIA) for types of processing that are likely to result in a high risk to the rights and freedoms of data subjects.

10.2 The University shall have in place appropriate processes to enable it to carry out Data Protection Impact Assessments where necessary. Data Protection Impact Assessments shall be carried out in consultation with the Information Compliance Manager, DPO and other relevant individuals or stakeholders as appropriate.

11 Personal Data Breaches

11.1 The University shall have in place appropriate processes for the reporting and handling of personal data breaches. Such processes shall provide that all personal data breaches must be reported immediately to the Information Compliance Manager, who will promptly inform the DPO.

11.2 The DPO or, in their absence, their nominee will decide whether any personal data breach is reportable to the Information Commissioner's Office or to the relevant data subjects. The DPO and/or the Information Compliance Manager will also advise relevant staff and authorised University representatives on action that is required internally and provide guidance to assist with mitigating risk of future breaches.

12 Training and Awareness

12.1 The University is committed to ensuring that its staff and relevant authorised University representatives undertake appropriate training on data protection. The University shall have in place an appropriate training course on data protection, which staff shall complete upon induction and thereafter as required. Such training course may also be undertaken by relevant authorised University representatives, as appropriate. The Information Compliance Manager may also provide bespoke training and advice to staff and authorised University representatives upon request.

12.2 The University shall make available resources, tools, advice and information (including links to relevant external advice and guidance such as that published by the Information Commissioner's Office) relating to data protection to enable staff and relevant University representatives to comply with the Data Protection Laws. Further information is available on the ICO website: https://ico.org.uk/

APPENDIX: DATA PROTECTION DEFINITIONS

(Data) controller determines the purposes for which personal data is processed. The controller is ultimately responsible for the personal data.

(Data) processor is any individual or organisation who/which processes personal data on behalf of and according to the purposes defined by the controller.

Data protection laws means any applicable legislation in the UK relating to the processing of personal data and includes the Data Protection Act 2018, the UK General Data Protection Regulation and, in certain circumstances, the EU General Data Protection Regulation 2016/679

Data subject is the living individual who the personal data is about.

Personal data is information which can be used to identify a living individual. As well as images, names and contact details, it can also include numerical or statistical information from which a person can be indirectly identified

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (including breaches that are the result of both accidental and deliberate causes).

Processing means any operation or set of operations performed upon personal data, whether or not by automatic means, including collecting, recording, storing, using, analysing, combining, disclosing or deleting personal data.

Special category data is 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 person, data concerning health or data concerning a person's sex life or sexual orientation. Criminal offence data falls out of scope of this definition as it is covered elsewhere in the Data Protection Laws, but it should be treated the same as special category data.