Data Protection Policy

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 A**.

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 Information Governance Lead 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 Governance Officer.

3.4 The Information Governance Group is responsible for overseeing the implementation of improvements identified to support the Information

Governance Policy through the Information Governance Programme, including with regard to Data Protection law and the management of associated risks.

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

- Managing and responding to information rights requests including providing support for the investigation of complaints, reviews of decisions and appeals; providing advice, guidance, training, awareness-raising 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 reviewing Data Protection Impact Assessments, Data Processing, Data Sharing and International Data Transfer Agreements and Transfer Risk Assessments.

  Developing and updating information governance policies, procedures, guidance and other material to enable best practice.

- Maintaining and developing the University's Publication Scheme under Freedom of Information legislation.

- Working collaboratively with IT, Information Security and Procurement colleagues to assess requests for new software and contracts.

- Monitor and report on data incidents and support investigation and notifications to the regulator.

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 Students and Applicants Privacy Notice 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 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 or clear regulation which requires the personal data to be processed;

- processing is necessary 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 Governance Officer. 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 this must be documented. The University's privacy notices broadly outline the legal bases for processing carried out as part of the University's standard functions. Further information can be found in Appendix B 'Approved Policy Document'.

6.4 The UK GDPR gives extra protection to the personal data of offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings **(Criminal Offence Data)** requiring the University to identify a specific condition for processing this information and these are set out in Appendix B. The University's Safeguarding Policy provides guidance on protecting welfare and the process to follow in the event of a concern or incident, alongside the Disclosure and Barring Scheme which assesses applicants' suitability for positions of trust (see Disclosure and Barring Scheme (DBS)) and the Declaring a Criminal Conviction Policy and Procedures for Applicants and Students Declaring a Criminal Conviction which explains the process to follow when declaring this data.

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 several 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 Governance Officer 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 regulations**: the United Kingdom has determined that the third country to which the personal data is transferred ensures an adequate level of protection for people's rights and freedoms; 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; or

- **exception**: one of the eight exceptions applies: explicit consent, contract (entering into or obligations relating to a contract), public interest, legal claims, protecting someone's vital interests, public register related, one-off transfer necessary to meet compelling legitimate interests.

And where applicable, a Transfer Risk Assessment has been undertaken.

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 Governance Officer, 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 Governance Officer, who will promptly inform the DPO.

11.2 The DPO or, in their absence, their nominee will decide in consultation with the University Secretary 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 Governance Officer 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 Governance Officer 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 A

DATA PROTECTION DEFINITIONS

Criminal Offence Data includes personal data relating to criminal convictions and offences or related security measures. It covers a wide range of information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings and may also include personal data about unproven allegations, the absence of convictions and conditions or restrictions placed on an individual.

(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 Impact Assessment (DPIA) is a process designed to help organisations systematically analyse, identify, and minimise the data protection risks of a project or plan.

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.

Transfer Risk Assessment (TRA) is a process required under the UK GDPR to evaluate the risks associated with transferring personal data to a country outside the UK, in the absence of UK Adequacy Regulations. Adequacy Regulations indicate that the jurisdiction provides a level of data protection comparable to that of the UK.

Appendix B

Bath Spa University: Appropriate Policy Document

The University processes special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special category data
Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- 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.

Criminal offence data
Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

This policy document
Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices: Privacy notices.

Conditions for processing special category and criminal offence data
We process special categories of personal data under the following UK GDPR Articles:

i. Article 9(2)(a) – explicit consent. In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information we receive from our students who require a reasonable adjustment to access our services.

ii. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the University or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences and checking if individuals are entitled to work in the UK.

iii. Article 9(2)(c) – where 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.
Examples of our processing include where an individual needs emergency medical services but is unconscious or otherwise incapable of giving consent.

iv. Article 9(2)(f) – if processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Examples of our processing include processing relating to litigation in relation to an employment tribunal or personal injury claims.

v. Article 9(2)(g) – for reasons of substantial public interest.

Examples of our processing include the information we seek or receive as part of establishing the immigration status of students.

We process criminal offence data under Article 10 of the GDPR.

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Processing requiring an Appropriate Policy Document
Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an Appropriate Policy Document (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the Appropriate Policy Document for Bath Spa University. It demonstrates that the processing of special category and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Description of data processed
We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any trade union. Further information about this processing can be found in our staff privacy notice.

Our processing for reasons of substantial public interest relates to the public good, or what is in the best interests of society. This includes ensuring equality or preventing fraud. Further information about this processing can be found in our privacy notice.

We also maintain a record of our processing activities in accordance with Article 30 of the GDPR.

Schedule 1 conditions for processing
We process Special Category Data for the following purposes in Part 1 of Schedule 1:

Paragraph 1(1) employment, social security and social protection.

We process special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 8(1) equality of opportunity or treatment
- Paragraph 9(1) racial and ethnic diversity at senior levels
- Paragraph 10(1) preventing or detecting unlawful acts
- Paragraph 11(1) and (2) protecting the public against dishonesty
- Paragraph 12(1) and (2) regulatory requirements relating to unlawful acts and dishonesty
- Paragraph 14(1) and (2) preventing Fraud
- Paragraph 15(a) and (b) suspicion of terrorist financing or money laundering
- Paragraphs 18(1) to (4) safeguarding children and individuals at risk
- Paragraph 19(1), (2) and (3) safeguarding of economic well-being of certain individuals
- Paragraphs 20(1) to (7) insurance
- Paragraphs 21(1) to (4) occupational pensions
- Paragraph 24(1) and (2) disclosure to elected representatives

Criminal offence data
We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:
Paragraph 1 – employment, social security and social protection

Procedures for ensuring compliance with the principles

Accountability principle
We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Officer who reports directly to our highest management level;
- Taking a 'data protection by design and default' approach to our activities;
- Maintaining documentation of our processing activities;
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors;
- Implementing appropriate security measures in relation to the personal data we process;
- Carrying out data protection impact assessments for our high risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (a): lawfulness, fairness and transparency
Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this policy document.

Our processing for reasons of substantial public interest relates to the public good, or what is in the best interests of society. This includes ensuring equality or preventing fraud. Further information about this processing can be found in our privacy notice.

Our processing for the purposes of employment relates to our obligations as an employer.

Principle (b): purpose limitation
We process personal data for purposes of substantial public interest as explained above where it is necessary for complying with or assisting another to comply with a regulatory requirement to establish whether an unlawful or improper conduct has occurred, to protect the public from dishonesty, preventing or detecting unlawful acts or for disclosure to elected representatives.

We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): data minimisation
We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our

purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Principle (d): accuracy
Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle (e): storage limitation
All special category data processed by us for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in our retention schedule. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security)
Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures.

Our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

Retention and erasure policies

Our retention and erasure practices are set out in our retention schedule.

Appropriate Policy Document review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed at the same time as the overarching Data Protection Policy or revised more frequently if necessary.

Additional special category processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices.

Document Details

Responsible Office: Governance, Legal & Compliance

Responsible Officer: University Secretary

Approving Authority: Audit Committee

Date of latest approval: June 2022

Amended (if applicable): 12 March 2025 (technical/minor editorial updates)

Effective Date: June 2022

Related Policies and Procedures:

AI Policy

Declaring a Criminal Conviction Policy and Procedures

Information Governance Policy

Mobile and Remote Working Policy

Privacy notices

Records Management Policy

Records Retention Policy and Retention Schedule

Regulations for the Use of Computer Facilities

Research Data Policy

Safeguarding Policy

Personal Data Breach Procedure

Data Subject Access Request Procedure

Supersedes: v. May 2018

Next review due: June 2027