Data Protection Policy

Information Governance

This document can only be considered valid when viewed via the University website. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one on the University website. Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Contents:

1. Introduction

1.1 The UK General Data Protection Regulation (referred to as the UK GDPR) and the Data Protection Act 2018 (referred to as the DPA) place specific responsibilities on organisations which process personal data and provide individuals to whom that data relates with certain rights.

1.2 The University of Bradford, in order to conduct its business, necessarily handles substantial amounts of personal data, a great deal of which falls into the special categories (for definitions of such terms please refer to section 3 below). The University must therefore ensure that this processing is performed in accordance with the UK GDPR and DPA but in doing so, has to also ensure that its business processes remain workable.

1.3 The University takes its duties with respect to personal data very seriously, and is committed to ensuring that it complies with the UK GDPR and DPA.

1.4 The University also needs to abide by the data protection principles to maintain the confident and trust of the individuals and organisations that it collaborates with.

1.5 The objectives of this policy are to establish:

- The University's commitment to data protection and to its compliance with the UK GDRP and DPA;
- the role of the Data Protection Officer; and
- general principles and responsibilities in relation to the processing of personal data.

2. Scope

2.1 This policy applies to all University employees, associates, students, contractors and others who process personal information on the University's behalf and in the course of their duties, responsibilities and studies.

3. Glossary

3.1 All specific terms in this Policy are as defined by Article 4 of the UK GDPR or elsewhere in the UK GDPR or DPA. The following summarises those and other definitions:

- Controller: an organisation (or person) which determines the purposes and means the of the processing of personal data.
- Data protection legislation; UK GDPR, DPA and supporting instruments, regulations and codes of practice.
- Data subject: an identifiable natural living person.
- DPA: the Data Protection Act 2018, c. 12, as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019).
- Personal data: any information relating to an identified or identifiable person ('data subject').
- Privacy notice: a document fulfilling the requirements of Articles 13 and 14 of the UK GDPR which lay out data subjects' rights to be informed about the processing of their personal data (including the purposes for which personal data in collected and used, how it is used and disclosed, how long it is kept, and the controller's legal basis for processing).
- Processing: any activity performed on personal data including collecting, recording, organising, structuring, storing, adapting, retrieving, consulting, use, disclosure, combination, erasure and destruction.
- Processor: an organisation (or person) which processes personal data on behalf of a controller.
- Record of processing activity; a formal record of how personal data is processed covering areas such as processing purposes, data sharing and retention. Full details of what is required are listed in Article 30 of the UK GDPR.
- Special categories of personal data; as defined by Article 9 of the UK GDPR:
    - Personal data revealing:
        - Racial or ethnic origin;
        - Political opinions;
        - Religious or philosophical beliefs;

        - Trade union membership;
    - The processing of genetic data;
    - Biometric data processed for the purpose of uniquely identifying a data subject;
    - Data concerning health; and
    - Data concerning a person's sex life or sexual orientation
- UK GDPR: the UK General Protection Regulation (i.e. EU GDPR (Regulation (EU) 2016/679 (General Data Protection Regulation) as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019).

4. Responsibilities

Executive Board

4.1 The University Secretary will, on behalf of the Executive Board, ensure that a Data Protection Officer (DPO) is appointed to maintain oversight of the University activities falling within the scope of the data protection legislation and accepted good practices.

4.2 The Executive Board, following the advice and guidance of the University Secretary, will ensure that the office of DPO has the resources, expertise and authority to carry out the tasks outlined in this policy.

4.3 The DPO will not receive any instruction regarding the exercise of those tasks nor will be dismissed or penalised for performing the tasks outlined below.

Data Protection Officer

4.4 The DPO shall be involved, properly and in a timely manner, in all issues which relate to the protection of personal data and shall report on matters relating to compliance with data protection legislation to the Executive Board with regular reports and in the event of exceptional events.

4.5 As required by Article 39 of the UK GDPR, the office of DPO will as a minimum be responsible for the following tasks:

- To inform and advise the University and its employees of their obligations in respect of compliance with data protection legislation;
- To monitor compliance with data protection legislation and with the University's policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- To provide advice relating to, and monitor performance of, data protection impact assessments;
- To cooperate with and act as the contact point for the Information Commissioner's Office.

4.6 The DPO shall ensure that the information asset registers and the record of processing activities are maintained.

4.7 The DPP shall ensure privacy notices are in place for all processing of personal data.

4.8 The DPO shall, in the performance of their tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

4.9 The DPO will serve as the principle contact in the event of any suspect or actual breach of the data protection policy, will be involved in any investigation and be consulted in relation to any reports provided the Executive Board or other parties.

Information Asset Owners

4.10 Information Asset Owners (IOAs) are those senior managers heading faculties and professional services. The IAO is responsible for ensuring that business information is handled and managed appropriately within their faculties or professional service. This must include all personal data used by the University.

4.11 IAOs must determine (both initially and in the case of any significant changes) what data is captured, used and stored, who needs to use it and why and how long it should be kept. IAOs must advise the DPO of data processed and held.

4.12 IAOs are also accountable for ensuring that:

4.12.1 staff and students within their areas are aware of the Dat Protection Policy;

4.12.2 adequate resources are made available to ensure that their staff (and students) are able to work in accordance with this policy;

4.12.3 all new staff (and students), be they permanent, temporary, employed by the University or contractors or agency staff are all inducted appropriately in terms of data protection and undertake the specified levels of training; and

4.12.4 the business processes and practices in their area comply with this Policy.

Line managers

4.13 Line managers are responsible for the day-to-day implementation and must make sure that members of staff are aware of this policy and University procedures relating to the correct handling of personal data.

Employees

4.14 All employees whether directly handling personal data or not must comply with data protection legislation and University procedures.

4.15 All employees must also complete all mandatory training provided by the University.

4.16 Employees must only use personal data in connection with legitimate University business or as instructed by their line manager.

4.17 Employees must not use any personal data to which they have access for personal or other non-University related purposes.

4.18 A member of staff must not access or amend any record or data which relates to, or is about, themselves.

4.19 Employees must report any breaches or suspected breaches in accordance with the University's data breach reporting procedures.

Students

4.20 All students who process personal data in the course of their studies must comply with this policy and any other policies and procedures which may be in place for their programme of study including the Ethics Policy and related documents.

4.21 Students undertaking research involving people and the processing of personal data must ensure that all such processing is in accordance with the requirements of data protection legislation. Research supervisors are responsible for ensuring that post-graduate research students are aware of and follow University policy.

4.22 Where necessary students shall be required to undertake training in the principles of the data protection legislation and the University processes designed to ensure compliance with the legislation.

5. General principles / Policy statements

Commitment to Data Protection

5.1 The University is committed to complying with the data protection legislation and good practice including:

5.1.1. Registering as a Controller with the Information Commissioner;

5.1.2. Processing personal data lawfully;

5.1.3. Processing personal data only where there is a demonstrable organisational purpose;

5.1.4. Processing only the amount of personal data required for the relevant organisational purpose;

5.1.5. Processing of personal data shall be restricted to those with a demonstrable need to process it;

5.1.6. Personal data shall be retained no longer than necessary and a schedule of retention periods or different categories of information shall be maintained;

5.1.7. The publication of privacy notices for all processing of personal data;

5.1.8. Maintaining a record of processing activity;

5.1.9. Respecting individuals rights in respect of their data;

5.1.10. Keeping personal data secure;

5.1.11. Transferring any information to third parties and / or overseas only where there are formal arrangements to ensure adequate protection;

5.1.12. Adopting a privacy by design and by default approach and undertaking data protection impact assessments; and

5.1.13. Reporting breaches of data protection, as required, to the Information Commissioner.

Data Subject Rights

5.2 The DPO will publish guidance on the website advising how data subjects may exercise their rights in respect of their personal data held by or on behalf of the University.

5.3 Where it is feasible to do so, individual faculties and professional services should provide data subjects with informal access to the personal data they hold.

5.4 A formal centralised Subject Access Request process for a data subject's general right of access to personal data held by the University shall be managed by the Legal and Governance Department. Requests can be made via data-protection@bradford.ac.uk

5.5 The University shall ensure it is satisfied as to the identify of the data subject when they make such request and that it received proof of authorisation where requests are made on the behalf of the data subject by a third party.

6. Implementation

6.1 The Policy will be uploaded onto the University website and communicated to the University community.

7. Enforcement of this Policy and Sanctions

7.1 Compliance with this policy is the responsibility of all members of staff, associates, students, contractors and other third parties who process personal information on the University's behalf and in the course of their duties, responsibilities' and studies.

7.2 Anyone found to be acting in breach of this policy or who is negligent in their responsibilities to enforce it may be subject to disciplinary or capability procedures.

7.3 In serious cases, breaches of this Policy may be grounds for invocation of the Staff Capability and / or Disciplinary Policy and Procedure, and in the case of students, the Academic Misconduct Regulations, Fitness to Practice and / or Student Disciplinary Regulation and Procedure.

7.4 Any questions about the interpretation or operation of this policy should be referred to the Data Protection Officer.

8. Monitoring and Review

8.1 The impact of this Policy shall be reviewed by the Data Protection Officer.

8.2 This Policy shall be reviewed every two years from the date of approval.

9. Related Policies and Standards

- Information Security Policy and subsidiary policies
- Data Breach Procedure
- Data Protection Impact Assessment Procedure
- Privacy Notices
- Regulation on the appropriate use of University IT services
- Records Retention and Disposal Policy
- Staff Capability Policy and Procedure
- Staff Disciplinary Policy
- Student Disciplinary Regulation and Procedure
- Academic Misconduct Regulations
- Fitness to Practise Procedure

10. Document and version control information:

Version control information heading	Details
Owner	University Secretary, Legal & Governance
Author	Assistant Head (Student Conduct, Risk and Information Governance), Legal & Governance
Approved by	Version 2.3 (minor updates from v2.1) presented to Executive Board for approval 21 June 2023.
Date of approval of this version	21 June 2023
Next review date	1 July 2024
Version number	v2.3
Applicable statutory, legal, or national best practice requirements	UK General Data Protection Regulation Data Protection Act 2018
Equality impact assessment completion date	16 May 2018