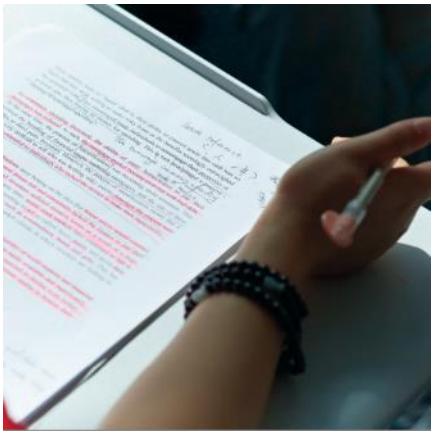
UNIVERSITY of BRADFORD

Data Protection

# Data Protection Policy



UNIVERSITY of BRADFORD

# Version Control

| | |
|---|---|
| Policy Number: | DP1 |
| Approved by: | Deputy Vice Chancellor (Operations), University Secretary and Director of Planning, Legal and Governance, Chief Information Officer on behalf of Executive Board as agreed on 14 March 2018 (Minute EB 170.17.18) |
| Date Approved: | 3 September 2018 |
| Next Review Date: | May 2020 |
| Version Number: | V2.0 |
| Applicable Statutory, Legal or National Best Practice Requirements: | General Data Protection Regulation<br>Data Protection Act 2018 |
| Equality Impact Assessment Completion Date: | 16 May 2018 |

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.

UNIVERSITY of BRADFORD

## Contents


1 Introduction ..... 4

2 Scope ..... 4

3 Glossary ..... 4

4 Responsibilities ..... 5

Executive Board ..... 5

Data Protection Officer ..... 6

Information Asset Owners ..... 7

Senior Managers ..... 7

Line Managers ..... 7

Employees ..... 7

Students ..... 8

5 General Principles ..... 8

Commitment to Data Protection ..... 8

Data Subjects Rights ..... 9

6 Implementation ..... 9

7 Enforcement of this Policy and Sanctions ..... 9

8 Monitoring and Review ..... 10

9 Related Policies and Standards ..... 10

UNIVERSITY of BRADFORD

# 1 Introduction

1.1 The General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018) 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 DPA 2018 and GDPR 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 GDPR and DPA 2018.

1.4 The University also needs to abide by the data protection principles to maintain the confidence 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 General Data Protection Regulation and Data Protection Act 2018;
- the role of 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 or elsewhere in the GDPR or DPA 2018. The following summarises those definitions:

- personal data: any information relating to an identified or identifiable person ('data subject').

- special categories: as defined by Article 9, personal data revealing:
  - racial or ethnic origin;
  - political opinions;
  - religious or philosophical beliefs;
  - trade union membership;
  - health;
  - natural person's sex life or sexual orientation;

  and genetic data and biometric data processed for the purpose of uniquely identifying a data subject.
- data subject: an identifiable person.
- processing: any activity performed on personal data such as collecting, recording, organising, structuring , storing, adapting, retrieving, consulting, use, disclosure, combination, erasure and destruction
- controller: an organisation (or person) which determines the purposes and means of the processing of personal data.
- processor: an organisation (or person) which processes personal data on behalf of a controller;
- privacy notice: a document made available to data subjects which explains the purposes for which personal data is collected and used, how it is used and disclosed, how long it is kept, and the controller's legal basis for processing. Full details of what is required in a privacy notice is listed in Articles 13 and 14 of the GDPR;
- 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 GDPR.

3.2 The term *data protection legislation* shall be used to refer to the General Data Protection Regulation and Data Protection Act 2018 and supporting instruments, regulations and codes of practice.

# 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 officers will not receive any instructions 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, 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.
- to maintain information asset registers and the record of processing activities; and
- to ensure privacy notices are in place for all processing of personal data.

4.6 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.

4.7 The DPO will serve as the principal contact in the event of any suspected or actual breach of the data protection policy, will lead any investigation and report the finding to the Executive Board and other parties.

## Information Asset Owners

4.8 Information Asset Owners (IAOs) are those senior managers responsible at a University level for ensuring that business information is handled and managed appropriately. This must include all personal data used by the University.

4.9 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. IAO's mut advise the DPO of data processed and held..

## Senior Managers

4.10 All Senior Managers (i.e. DVCs, PVCs, Directors and Deans) are accountable for ensuring that staff and students within their areas

4.10.1 are aware of the Data Protection Policy;

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

4.10.3 that 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;

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

## Line Managers

4.11 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

4.12 All employees whether directly handling personal data or not must complete all mandatory training and comply with data protection legislation and University procedures.

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

### Students

4.14 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 in place for their programme of study.

4.15 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 PGR students are aware of and follow University policy.

4.16 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

### Commitment to Data Protection

5.1 The University is committed to complying with 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 of 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 all 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 Subjects 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 Individual Faculties, Directorates and Services should provide access at a local level to personal data wherever it is feasible to do so.

5.4 Nevertheless a formal centralised Subject Access process shall exist to provide for a data subject's general right of access to their personal data held by the University (via data-protection@bradford.ac.uk).

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

## 6 Implementation

6.1 The Policy will be uploaded onto the University website.

6.2 The Policy will be communicated in the weekly University staff briefing and through other channels.

## 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 Data Protection 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 Practise 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
- Information Classification and Handling Policy
- Data Breach Procedure
- Data Protection Impact Assessment Procedure
- Privacy Notice Procedure
- Regulation 21 – ICT Regulations
- Records Retention and Disposal Policy
- Privacy Policy
- Staff Capability Policy and Procedure
- Staff Disciplinary Policy
- Regulation 28 – Student Disciplinary Policy