Teaching Intensive, Research Informed

DATA PROTECTION POLICY

(General Data Protection Regulation)

POLICY STATEMENT

The University intends to fully comply with all requirements of the Data Protection Act 1998 ('Act') and from 25 May 2018 with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') in so far as it affects the University's activities.

At the date of approval 6 February 2018, the Data Protection Bill was going through Parliament and it was intended that it would replace the Data Protection Act 1998, and supplement the General Data Protection Regulation by addressing those personal data processing activities that are not addressed by the General Data Protection Regulation.

SCOPE

This Data Protection Policy:

- Covers the processing of all personal information whose use is controlled by the University of Bolton.
- Covers all personal information handled, stored, processed or shared by the University whether organised and stored in physical or IT based record systems.
- Applies to all staff, applicants, students, contractors, partnership organisations and partner staff of the University.

INTRODUCTION

The University needs to collect and use data for a number of purposes about its staff, applicants, students and other individuals who come into contact with the University. In collecting and using this data, the University is committed to protecting an individual's right to privacy with regard to the processing of personal data and this policy has been implemented to support this commitment.

This policy sets out the rules that all University of Bolton staff, students, contractors, partnership organisations and partner staff who process or use any personal information on behalf of the University are subject to in order to ensure that the University is compliant with its data protection obligations.

The Act and, from 25 May 2018, the GDPR govern the collection, holding, processing and retention of all personal data relating to living individuals. The purpose being to ensure that those organisations and individuals, who collect, store and use that data do not abuse it, and process the data in accordance with the following Data Protection Principles that personal data shall:

i) be processed lawfully, fairly and in a transparent manner;

ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

iii) be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

iv) be accurate and kept up to date;

v) not be kept for longer than is necessary for those purposes;

vi) be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The University and its staff, students, contractors, partnership organisations and partner staff that process or use personal data on behalf of the University must comply and be able to demonstrate compliance with these principles and ensure that they are followed at all times. The Act and the GDPR covers ***all personal data that is held electronically, including databases, email and the Internet as well as manual filing systems eg. paper records.***

POLICY STATEMENTS

1. Policy Status

This policy is not part of the formal contract of employment, but it is a condition of all employment contracts that employees will follow the rules and policies created by the University from time to time. Failure to follow the policy can result in disciplinary action being taken.

All partner and contractor agreements must include appropriate data protection clauses relating to the University's Data Protection Policy and approved procedures for recording, using and/or processing personal data.

2. Responsibilities

The legal responsibility for compliance lies with the University who is the 'data controller' registered as such with the Information Commissioner's

Office (Registration Number No. Z5888188) and any 'data processor' that processes personal data on behalf of the University.

Responsibility for compliance is delegated to senior management members and data protection champions within the Faculties, Academic Schools and Professional Support Services who are responsible for encouraging data processing best practice within the University. However, compliance with this policy is the responsibility of everyone within the University who processes personal information.

3. Lawful Basis for Processing

It is necessary for the University to collect, process and use student data in order to perform the contract between the student and the University in providing teaching and education support services and a condition of staff employment that they agree to the University processing certain personal information as part of the University's obligations.

Some processing activities may also be carried out under the following legal bases; a legal obligation, where it is necessary to protect the vital interests of a student or another party, where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or where it is necessary for legitimate interests to be pursued by the University or a third party. Where any of these legal bases do not apply, the consent of an individual to process their personal data will be sought.

In most cases, the University can only process personal information that is categorised as "sensitive personal data" under the Act or "special category personal data" under the GDPR with the explicit consent of the individual whom the data concerns; this includes information about an individual's racial or ethnic origin, political opinions, gender, religion and beliefs, sexual orientation, physical or mental health or trade union membership with the addition of genetic and biometric data under the GDPR.

"Sensitive personal data" or "special category personal data" may also be collected and processed by the University on the legal basis of, employment or social security/protection requirements, protecting the vital interests of the individual or another party, the exercise or defence of a legal claim, reasons of substantial public interest, purposes of medical or health care or where the information has been made public by the individual, including for the purpose of scientific, research or statistical purposes. Any processing will be proportionate and relate to the provision of services by the University.

4. Information Disclosure

The University requires all staff, students, contractors, partnership organisations and partner staff to be vigilant and exercise caution when asked to provide personal data held on another individual. In particular, they must ensure that personal information is not disclosed either orally or in writing to any unauthorised personnel.

5. Data Processing

As and when staff, students, contractors, partnership organisations and partner staff are required to collect personal data, they must adhere to the requirements of this policy and any applicable local guidelines.

Students may process personal data in connection with their studies. This applies whether or not those activities are carried out on equipment owned by the University and whether or not they are carried out on University premises. If they do, they should be advised to inform their tutor, who will make any necessary enquiries with the Data Protection Officer.

6. Data Security

All staff, students, contractors, partnership organisations and partner staff must ensure that any personal information, which they hold, is kept securely and that they take appropriate security precautions by seeking to ensure the following:

- Source documents are kept in a lockable cabinet or drawer or room;
- Computerised data is password protected;
- Personal information is not disclosed orally or in writing, or in any other way, intentionally or otherwise to any unauthorised personnel;
- Data kept on discs or data storage devices are stored securely and encrypted;
- Ensure individual passwords are kept confidential and are not disclosed to other personnel enabling log-in under another individual’s personal username and password;
- Logged on PCs are not left unattended where data is visible on screen to unauthorised personnel;
- Screensavers are used at all times;

- Paper-based records must never be left where unauthorised personnel can read or gain access to them.

When manual records are no longer required, they should be shredded or bagged and disposed of securely and the hard drives of redundant PCs should be wiped clean.

Off-site use of personal data presents a greater risk of loss, theft or damage and the institutional and personal liability that may accrue from the off-site use of personal data is similarly increased. For these reasons, staff and others should:

- only take personal data off-site when absolutely necessary and for the shortest possible time;
- take particular care when laptops or personal machines are used to process personal data at home or in locations outside of the University, they are kept secure at all times.

Different types of information require different security measures. Proper classification is vital to ensuring effective data security and management. The Information Classification Guidance at Appendix 1 determines how different types of information should be managed and is applicable to all information held by the University.

7. Information Asset Register

In order to understand and manage the risks to the University's information it is necessary for the University to keep and maintain an information asset register detailing the personal information that the University holds and processes in all areas of the University.

Responsibility for maintaining and keeping up-to-date schedules of the information asset register, which relate to the areas of activity in the University, shall be delegated to the Data Protection Champion of each area. The Data Protection Officer shall be custodian of the institutional information asset register, comprised of the consolidated schedules, and will undertake an annual review of the schedules with the Data Protection Champion.

8. Data Security Breaches

A personal data breach means ***'a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.***

All information security incidents and data breaches must be reported promptly so the risk to individuals, the University and others can be

contained and prevented where possible. Any personal data breach that is likely to result in a risk to an individual's rights and freedoms must be reported to the Information Commissioner's Office within 72 hours after becoming aware of the breach and if there is the likelihood of a high risk to an individual's rights and freedoms, report the breach to those that have been affected.

Any student, staff, contractor, partnership organisations, partner staff or individual that processes, accesses, uses or manages personal data on behalf of the University is responsible for reporting information security incidents and data breaches. Information security incidents and data breaches must be reported to the Data Protection Champion, Data Protection Officer at dpo@bolton.ac.uk, Head of Information Systems and Technology and Registrar following the Data Security Breach Management Procedure at Appendix 2.

All staff should be aware that any breach of the Data Protection Act 1998 and, from 25 May 2018, with the General Data Protection Regulation could result in the University's disciplinary procedures being instigated.

9. Rights of Individuals

Under the Act and the GDPR, an individual has the following rights:

i. To request access to information held about them, the purpose for which the information is being used and those to whom it is, has or can be disclosed to;

ii. To prevent data processing that is likely to cause distress or damage;

iii. To prevent data processing for direct marketing reasons;

iv. To be informed about the reasons behind any automatic decision made;

v. To seek compensation if they suffer damage as a result of any breach by the Data Controller;

vi. To take action to stop the use of, rectify, erase, or dispose of inaccurate information;

vii. To ask the Information Commissioner to assess if any personal data processing has not been followed in accordance with the data protection principles.

Under the GDPR, an individual has the following additional rights:

i. To be forgotten, that is their details to be removed from systems that the University uses to process personal data;

ii. To restrict the processing of personal data in certain situations;

iii. To seek compensation if they suffer damage as a result of any breach by a Data Processor;

iv. To object to the processing of personal data in certain situations for example, sending and receipt of direct marketing material;

v. To data portability - obtain a copy of their data in a commonly used electronic form in order to provide it to other organisations;

vi. To object to automated decision making and profiling – object to decisions made by automated means without human intervention in certain circumstances;

vii. To withdraw consent where that is the legal basis of the University's processing personal data.

10. Access to Personal Data

Subject to exemptions, any individual who has personal data kept about them at the University has the right to request in writing a copy of the information held relating to the individual in electronic format and also in manual filling systems. Any person who wants to exercise this right should in the first instance make a written request to the University, using the University's 'Subject Access Form'.

Under the Act, the University will make an administrative charge of £10 each time that a request is made.

After receipt of a written request, the fee and any information needed as proof of identity of the person making the request, the University will ensure that the individual receives access within 40 calendar days, unless there is a valid reason for delay or an exemption is applicable.

Under the GDPR, the University will provide the information free of charge. However, a fee may be charged when a request is manifestly unfounded, excessive or repetitive taking into account the administrative costs of providing the information or the University may refuse to respond to the request. A fee may also be charged for further copies of the same information.

After receipt of a written request, the fee (if applicable) and any information needed as proof of identity of the person making the request, the University will ensure that the individual receives access within 30 calendar days, unless there is a valid reason for delay or an exemption is applicable.

An individual can make a subject access request via a third party, including by a solicitor acting on behalf of a client. In these cases and prior to the disclosure of any personal information, the University would need to be satisfied that the third party making the request is entitled to act on behalf of the individual and would require evidence of this entitlement.

Whilst there is no limit to the number of subject access requests an individual can make to any organisation, the University is not obliged to comply with an identical or similar request to one already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

11. Direct Marketing (the communication by whatever means of any advertising or marketing material which is directed to individuals)

An individual has the right to prevent his/her personal data being processed for direct marketing. An individual can, at any time, give written notice to stop (or not begin) using their personal data for direct marketing. Any individual can exercise this right, and if the University receives a notice then it must comply within a reasonable period.

12. Accuracy of Data

Staff are responsible for:

i) ensuring that any information they provide to the University relating to their employment is accurate and up to date;

ii) informing the University of any information changes, eg. change of address; and

iii) checking the information that the University may send out from time to time giving details of information kept and processed about staff.

Students must also ensure that all data provided to the University is accurate and up-to-date by either notifying Student Data Management at sdmenquiries@bolton.ac.uk or updating their student record online with any changes to their address or personal details.

The University cannot be held responsible for any errors unless the member of staff or student has informed the University about them.

13. Retention and Disposal of Data

The University is not permitted to keep personal information of either students or staff for longer than is required for its purpose. However, some data will be kept longer or in perpetuity to comply with statutory or funding body requirements.

Personal and confidential information will be disposed of by means that protect the rights of those individuals ie. shredding, disposal of confidential waste, secure electronic deletion.

14. Complaints

The University is dedicated to being compliant with the Act and, from 25 May 2018, the GDPR. Individuals, any member of staff, applicant or a student wishing to report concerns should, in the first instance, contact the University's Data Protection Officer who will aim to resolve any issue:

Data Protection Officer
The University of Bolton
Deane Road
Bolton
BL3 5AB

Email: dpo@bolton.ac.uk

If the individual, member of staff or student feels the complaint has not been dealt with to their satisfaction, he/she can formally complain to the Registrar.

The individual also has the right to complain to the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113
Internet: www.ico.org.uk

OTHER RELATED POLICIES

- Records Retention and Disposal policy
- Records Retention Schedule
- Student Privacy Notice
- Staff Privacy Notice
- Data Security Breach Management Procedure
- Information Classification Guidance
- Information Security Policy

- Library Code of Conduct
- Code of Practice for Ethical Standards in Research
- Human Resources Policies and Procedures
- Freedom of Information Act Publication Scheme
- Academic Policies, Procedures and Regulations
- Student Policies, Procedures and Regulations

LOCATION, ACCESS AND DISSEMINATION OF THE POLICY

Overall responsibility for the policy implementation rests with the Registrar. However, all staff and/or students are obliged to adhere to, support and implement this policy.

For useful information and advice on data protection contact: www.ico.org.uk

The following Officers will be responsible for providing advice to staff and students on the application of the policy to specific cases in the first instance:

- Data Protection Officer
- Data Protection Champions

This policy will be made available on the University website to all staff, applicants, students and external third parties.

TITLE OF POLICY: Data Protection Policy	
Policy Ref	VC/07/2015
Version Number	4.0
Version Date	December 2017
Name of Developer/Reviewer	Registrar (Developer) Contracts and Compliance Officer
Policy Owner (Group/Centre/Unit)	Vice Chancellor's Office
Person responsible for implementation (postholder)	University Registrar and Chief Operating Officer
Approving Committee/Board	Executive Board
Date Approved	
Effective from	
Dissemination method (eg website)	Website
Review Frequency	As and when required
Reviewing Committee	Executive Board
Consultation history (individuals/group consulted and dates)	
Document History (e.g. rationale for and dates of previous amendments)	Updated to reflect the General Data Protection Regulation.

APPENDIX 1

Information Classification Guidance

(see https://www.bolton.ac.uk/about/governance/documents/)

APPENDIX 2

Data Security Breach Management Procedure

(see https://www.bolton.ac.uk/about/governance/documents/)