DATA PROTECTION POLICY

POLICY STATEMENT

3. Lawful Basis for Processing

The University may only process personal data fairly and lawfully and for specified purposes to ensure that personal data is processed without prejudicing the rights and freedoms of data subjects.

In order to process non-special category personal data, processing activities must meet at least one of the following lawful bases:

consent of the data subject;

necessary for the performance of a contract with the data subject;

necessary due to a legal obligation;

necessary to protect someone's vital interests;

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.

It is a **criminal offence** under the Act to knowingly or recklessly:

handle personal data without the consent of the data controller;

procure or disclose the personal data of another person without the consent of the data controller; or

retain personal data, after it has been obtained, without the consent of the data controller.

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

The University is committed to data protection by design and default. 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 technical and organisational security precautions by seeking to ensure the following:

personal information is not disclosed orally or in writing, or in any other way, intentionally or otherwise to any unauthorised personnel (internally or externally);

source documents are kept in a lockable cabinet or drawer or room;

computerised data is password protected;

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 personal data is visible on screen to unauthorised personnel;

screensavers are used at all times;

have been affected. Failure to notify a breach when required to do so may result in the University incurring a significant fine.

if the data subject has objected to processing for direct marketing purposes;

if the processing is unlawful.

vii) to take action to stop the use of, rectify, erase or dispose of inaccurate

alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of the information that a data subject is entitled to receive.

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

The University is subject to certain rules and privacy laws when marketing to applicants, students, alumni and other potential users of University services.

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 are responsible for:

i) ensuring 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 by ing thei rdrber01 Tc 0D(of)5.1 ( )]TJTw any onaonc tyit.7

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 AND RELEVANT INFORMATION AND REGULATION

Student Privacy Notice

Staff Privacy Notice

Data Privacy Impact Assessment Guidance

Data Privacy Impact Assessment

Data Privacy by Design and Default Guidance

Information Security Policy

[This is not an exhaustive list.]

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.

The University reserves the right to change this policy at any time without notice so please

LE OF POLICY: Data Protection Policy	
icy Ref	VC/08/2018
sion Number	5.0
sion Date	18 June 2018
me of Developer/Reviewer	Contracts and Legal Compliance Adviser/DPO (Developer) Registrar (Reviewer)
icy Owner (Group/Centre/Unit)	Vice Chancellor's Office
son responsible for lementation (postholder)	Registrar Contracts and Legal Compliance Adviser/DPO
proving Committee/Board	Executive Board
e Approved	18 June 2018
ective from	18 June 2018
semination method (eg website)	Website
view Frequency	As and when required.
viewing Committee	Executive Board
nsultation history dividuals/group consulted and es)	
cument History (e.g. rationale for dates of previous amendreW nBT	

APPENDIX 1

Information Classification Guidance

https://www.bolton.ac.uk/assets/Uploads/Information-Classification-Guidance-April-2018.pdf

APPENDIX 2

Data Breach Management Procedure

https://www.bolton.ac.uk/assets/Uploads/UoB-Data-Breach-Management-Procedure-April-2018.pdf