DATA PROTECTION POLICY

POLICY STATEMENT

The University intends to fully comply with all requirements of the Data Protection Act 1998 ('Act') in so far as it affects the University's activities.

SCOPE

This Data Protection Policy:

- Covers the processing of all personal information whose use is controlled by the University of Bolton and defined in the University's Data Protection Notification (Registration No Z5888188).
- 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, 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, 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. The University must comply with the Act.

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 obligations under the Act.

The Act governs the collection, holding, processing and retention of all personal data relating to living individuals. Its 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 eight Data Protection Principles that personal data shall:

i) be processed fairly and lawfully and shall not be processed unless certain conditions are met;

ii) be obtained only for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes;

iii) be adequate, relevant and not excessive for those purposes;

iv) be accurate and kept up to date;

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

vi) be processed in accordance with the data subject's rights under the Act;

vii) be kept safe from unauthorised access, accidental loss or destruction;

viii) not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

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 with these principles and ensure that they are followed at all times. As stated, ***the Act covers all personal data that is held electronically, including databases, email and the Internet as well as some paper records.*** The paper records that are subject to the Act are those that are contained in a 'relevant filing system' where the data is organised and structured.

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 agreements must include appropriate 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 with the Act lies with the University who is the 'data controller' under the Act and is registered as such with the Information Commissioner's Office. Responsibility for compliance is

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

3. Individual Consent

In most cases, the University can only process personal data with the consent of the individual whom the data concerns. If the information is sensitive personal data, explicit consent may be needed. However, it is a condition of student enrolment and of staff employment that they agree to the University processing certain personal information as part of the University's statutory obligations. See also the document 'Processing Your Personal Data'.

The University may process some information that is categorised as "sensitive personal data"; this includes information about an individual's racial or ethnic origin, gender, religion and beliefs, sexual orientation, physical or mental health, trade union membership and criminal convictions, charges or proceedings. This information may be required to comply with certain government or funding body regulations, to ensure safety or to meet the requirements of the University's policies and procedures.

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, which includes family members, friends, government bodies and in certain circumstances the police, without the express prior consent of the relevant individual.

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. 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 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 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.

7. Rights of Individuals

Under the Act, 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 of the Act 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 Act.

8. Access to Personal Data

Subject to exemptions, the Act gives any individual who has personal data kept about them at the University the right to request in writing a copy of the information held relating to the individual in electronic format and also in some 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'. 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.

The Act does not prevent an individual making 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 the Act does not limit 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.

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

Under the Act 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.

Any marketing campaign should be permission-based with a clear explanation of what an individual's details will be used for and a simple way should be included for an individual to opt out of marketing messages.

10. 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 their School Office 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.

11. 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.

12. Complaints

The University is dedicated to being compliant with the Act. Individuals, any member of staff or a student wishing to report concerns relating to the Act should, in the first instance, contact the following member of staff who as the University's Data Protection Officer will aim to resolve any issue:

Contracts & Compliance Officer (Data Protection Officer)
The University of Bolton
Deane Road

Bolton
BL3 5AB

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.

OTHER RELATED POLICIES

- 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:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113
Internet: 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:

- Contracts & Compliance Officer (Data Protection Officer)
- Head of Information Systems and Technology
- Manager of Student Services
- Senior Administration Manager (On Campus)
- Senior Administration Manager (Off Campus)

- Head of Quality Systems
- Director of Human Resources
- Registrar

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

TITLE OF POLICY: Data Protection Policy	
Policy Ref	VC/07/2015
Version Number	3.0 (Technical update only)
Version Date	July 2015
Name of Developer/Reviewer	Registrar (Developer) Contracts and Compliance Officer (Technical Update Reviewer)
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 with change in personnel contact details and links to related policies. This version has had technical changes only to reflect changes to role holder and organisational structure – no committee approval required as technical changes only