DATA PROTECTION POLICY

POLICY STATEMENT

The University intends to fully comply with all requirements of the Data Protection Act 2018 ('Act') and the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') in so far as they affect the University's activities. This policy sets out how the University manages those requirements.

The Act shall supplement the GDPR by addressing those personal data processing activiti

The Act and 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) be 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 systemseg. 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 familiarise themselves with and follow the policies and procedures of the University from time to time. Failure to follow the policy can result in disciplinary action being taken.

Compliance with this policy is a condition of the student contract to abide by the University's regulations, policies and procedures. 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' as registered with the Information Commissioner's Office (Registration Number No. 25888188) 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 Centres, Academic Schools and

Professional Support Services who are responsible for encouraging and facilitating 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

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 for reasons of public health;
- necessary for the purposes of medicine, the provision of health or social care.

Personal data relating to criminal conv1are.

- 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;
- paper-based records containing personal data 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 orbagged 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.

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

- re-identify de-identified personal data without the consent of the data controller who de-identified the personal data; or
- process personal data that has been re-identified without the consent of the data controller responsible for the de-identification.

The Information Security Policy, Internet Security Policy, Acceptable Use Policy and Guidance on Security with Mobile Devices must be read in conjunction with this policy.

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.

- if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- if the legal basis of processing is consent and that consent has been withdrawn and there is no other legal basis on which to process that personal data;
- if the data subject objects to processing where the legal basis is the pursuit of a legitimate interest or public interest and there is no overriding legitimate grounds or interest;
- 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 information;

viii) to object to automated decision making and profiling - object to decisions made by automated means without human intervention in certain circumstances;

ix) to be informed about the reasons behind any automatic decision made;

x) to prevent data processing that is likely to cause distress or damage;

xi) to seek compensation if they suffer damage as a result of any breach by the Data Controller or Data Processor;

xii) to ask the Information Commissioner to assess if any personal data processing has not been followed in accordance with the data protection principles; and

xiii) to data portability - obtain a copy of their data in a commonly usedelectronic form in order to provide it to other organisations.

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

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

APPENDIX 2

Data Breach Management Procedure

https://www.bolton.ac.uk/wp-content/uploads/2018/04/UoB-Data-Breach-Management-Procedure_April-2018.pdf