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 activities that are not addressed by the GDPR. The GDPR forms part of the data protection regime in the UK together with the Act and must be read alongside each other with the former prevailing.

SCOPE

This Data Protection Policy:

covers the processing of all personal information controlled by the University.

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.

covers the procedures to be followed by any student, staff, contractor, partnership organisation, partner staff or individual that processes, accesses, uses or manages personal data on behalf of the University in reporting information security incidents and data breaches to the University so it may comply with its legal obligation and ensure the risk to individuals, the University and others can be contained and prevented where possible. **See paragraph 8 Personal Data Security Breaches**.

INTRODUCTION

The University needs to collect and use data for a number of purposes about potential staff and students (applicants), current staff and students, former staff and 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 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 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)

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 to protect someone's vital interests;

necessary for f personal data is procul rract7-4(s.)] TJET(s a)15(7- /MC)-4(ik)6(l)5(i(s ca( )-

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 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

8. Personal Data Security Breaches

The University has a legal requirement to report certain types of personal data breach to the Information Commissioner's Office within **72 hours** of becoming aware of the breach, where feasible, and if there is the likelihood of a **high risk** to an individual's rights and freedoms, the breach must be reported to those that have been affected. Failure to notify a breach when required to do so may result in the University incurring a significant fine.

A personal data breach means _____

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

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 subj

TITLE OF POLICY: Data Protection Policy	
Policy Ref	VC/08/2018
Version Number	5.0
Version Date	June 2018
Name of Developer/Reviewer	Contracts and Legal Compliance Adviser/DPO (Developer) Registrar (Reviewer)
Policy Owner (Group/Centre/Unit)	Vice Chancellor's Office
Person responsible for implementation (	

APPENDIX 1

Information Classification Guidance

https://www.bolton.ac.uk/wp-content/uploads/2018/04/Information-Classification-Guidance-_April-2018.pdf

APPENDIX 2

Data Breach Management Procedure

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