Data Protection Policy

1. Policy Statement

1.1 The General Data Protection Regulation ('GDPR') effective on 25 May 2018 and as supplemented by a new Data Protection Act following the Assent of the Data Protection Bill ('Data Protection legislation'), replaces the Data Protection Act 1998 and sets out legislative requirements for organisations processing personal data (referred to under the Data Protection legislation as 'Data Controllers').

1.2 Data Protection legislation and the Freedom of Information Act 2000 are overseen, and enforced by the Information Commissioner's Office (ICO), who is an independent public body responsible directly to Parliament.

1.3 The University of Wolverhampton ('the University'), as a data controller, will be open and transparent when processing and using personal information by following the 6 Principles as set out in the Data Protection legislation:

Personal data shall be:

Principle 1: 'Lawfulness, fairness and transparency': processed lawfully, fairly and in a transparent manner in relation to the data subject;

Principle 2: 'Purpose Limitation': collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

Principle 3: 'Data Minimisation': adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Principle 4: 'Accuracy': accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

Principle 5: 'Storage Limitation': kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of appropriate technical and organizational measures in order to safeguard the rights and freedoms of data subjects;

Principle 6: 'Integrity and Confidentiality': processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;

Principle of Accountability: The Controller shall be responsible for, and be able to demonstrate compliance with the 6 Data Protection Principles.

2. Scope of Policy

2.1 This policy applies to all members of the University within the University group. For the purposes of this policy, the term "Staff" means all members of University staff including permanent, fixed term, and temporary staff, governors, secondees, any third party representatives, agency workers, volunteers, interns, agents and sponsors engaged with the University in the UK or overseas. This policy also applies to all members of staff employed by any of the University's subsidiary companies.

2.2 All contractors and agents acting for or on behalf of the University should be made aware of this policy.

2.3 The University Secretary is responsible for the operation of this policy.

3. Definitions

3.1 This policy applies to all personal and special category data processed and stored electronically[1] and manually (paper based) files[2]. It aims to protect and promote the rights of individuals ("Data Subjects") and the University.

3.2 "Personal Data" Any information which relates to a living individual who can be or may be identified from that information, for example: by reference to a person's name and address (postal and email)

(i) Date of birth
(ii) Statement of fact
(iii) Any expression or opinion communicated about an individual
(iv) Minutes of meetings, reports
(v) Emails, file notes, handwritten notes, sticky notes
(vi) CCTV footage if an individual can be identified by the footage
(vii) Employment and student applications
(viii) Spreadsheets and/or databases with any list of people set up by code or student/staff number
(ix) Employment or education history
(x) Online identifier, IP address

3.3 **"**Special category data**"** Any information relating to an individual's:

[1] This list is not exhaustive: PC's, Laptops, Tablets, Phones.
[2] Manual records are paper based and structured, accessible and form part of a relevant filing system (filed by subject, reference, dividers or content), where individuals can be identified and personal data easily accessed without the need to trawl through a file.

(i) Ethnicity
(ii) Gender
(iii) Religious or other beliefs
(iv) Political opinions
(v) Membership of a trade union
(vi) Sexual orientation
(vii) Medical history

3.4 "Criminal offence data" Any information relating to criminal allegations, convictions and offences. In order to process personal data relating to criminal convictions or offences, staff must have both a lawful basis for processing the information and either legal authority or official authority for processing.

3.5 "Data Subject" Any living individual who is the subject of personal data whether in a personal or business capacity/

3.6 The University recognises and understands the consequences of failure to comply with the requirements of Data Protection legislation may result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- Suspension/withdrawal of the right to process personal data by the Information Commissioners Office (ICO);
- Loss of confidence in the integrity of the University's systems and procedures;
- Irreparable damage to the University's reputation.

3.7 Where staff do not comply with this policy, the University may also consider taking action in accordance with the University's established Disciplinary Procedure.

4.0 Staff Obligations

4.1 Staff must not gain access to information that is not necessary to hold, know or process. Staff must not disclose personal information, without authorisation from the Data Protection Officer, unless necessary for standard academic, administrative or pastoral purposes. Staff must ensure that all information which is held is relevant and accurate for the purpose for which it is required. The information nmust not be kept for longer than is necessary and must be kept secure at all times.

Staff Checklist for Recording Data

- Is it really necessary to record the information?
- Is the information 'standard' or is it 'special category data'?
- If it is 'special category data', have you obtained the individual's explicit consent?
- Has the individual been made aware that this type of information about them will be processed?
- Do you have authority to collect/process the data and have you established the lawful grounds for processing this information?
- If yes, have you checked with the data subject(s) that the information

is accurate?

- Are you satisfied that the data is kept secure at all times?
- If you have not obtained the individual's consent, have you established which other lawful grounds for processing apply?
- If you are storing the data on a database, have you notified the Data Protection Officer and registered the database?
- How long do you need to retain the data and what processes have you established to ensure review/secure destruction?

4.2 Staff will ensure that all personal or special category information is anonymised as part of any evaluation of assets and liability assessments except as required by law.

4.3 Staff who manage and process personal or special category information will ensure that it is kept secure and where necessary confidential. Special category information will only be processed in line with the provisions set out in this policy.

4.4 Staff are responsible for notifying their line manager or the Data Protection and Freedom of Information Officer if they believe or suspect that this policy has or may not been adhered to.

4.5 Staff are responsible for notifying the University Secretary and the Data Protection and Freedom of Information Officer of any actual or potential data security breaches immediately upon discovery, in line with the University policy for Data Breach Incident Management.

5.0 University (Data Controller) Obligations

5.1 The University will follow Code of Practice issued by the ICO when developing policies and procedure in relation to data protection.

5.2 The University will ensure that Data Processing and/or Sharing Agreements are applied to all contracts and management agreements where the University is the data controller contracting out services and processing of personal data to third parties (data processors[3]). The University will ensure this agreement clearly outlines the roles and responsibilities of both the data controller and the data processor.

5.3 The University will adhere to and follow the 6 principles of data protection and the Privacy & Electronic Communications (PEC) Regulations when conducting surveys, marketing activities etc. and where the University collects, processes, stores and records personal data.

5.4 The University will not transfer or share personal information with countries outside of the European Economic Area (EEA) unless that country has a recognised adequate level of protection in place in line with the recommendations outlined in Data Protection legislation.

[3] "**data processor**", in relation to personal **data**, means any person (other than an employee of the **data controller**) who processes the **data** on behalf of the **data controller**.

5.5 The University will ensure all staff are provided with data protection training and promote the awareness of the University's data protection and information security policies, procedures and processes.

6.0 Data Subjects Rights

6.1 The University acknowledges individuals (data subjects) may exercise their rights under the Data Protection legislation, including the right to access any personal data held on our systems and in our files upon their request, the right to erasure, rectification and/or restriction of processing.

6.2 The University recognises that individuals have the right to make a request in writing and upon valid verification of their identity, may obtain a copy of their personal information, if held on our systems and files[4].

6.3 The University recognises that individuals, in certain circumstances only, may have the right to restrict data processing, or to object to automated decision making and stop direct marketing.

6.4 The University recognises that individuals, in certain circumstances only, may exercise the right to erasure and data portability.

6.5 The University will only share information in accordance with the provisions set out in the Data Protection legislation and where applicable the University will inform individuals of the identity of third parties to whom we may share, disclose or be required to pass on information to, whilst accounting for any exemptions which may apply under the Data Protection legislation.

7.0 Complaints

7.1 Individuals who wish to make a complaint relating to breaches of the Data Protection legislation and/or complaints that an individual's personal information is not being processed in line with this policy may do so in writing to the:
Data Protection & Freedom of Information Officer
Offices of the Vice Chancellor
University of Wolverhampton
MA214 Wulfruna Building
Wulfruna Street
Wolverhampton
WV1 1LY
or by emailing: dataprotection@wlv.ac.uk

7.2 If the individual is still dissatisfied after this course of action they may address their complaint in writing to the University Secretary at the following address:

[4] Individuals can access their personal data via a 'Subject Access Request' (SAR), full details can be found here: https://www.wlv.ac.uk/about-us/governance/legal-information/corporate- compliance/data-protection-policy/data-protection-subject-access/

University Secretary
Offices of the Vice Chancellor
University of Wolverhampton
MA216, Wulfruna Building
Wulfruna Street Wolverhampton
WV1 1LY

or by emailing: governance@wlv.ac.uk

8.0 Related Documents

8.1 Document Retention Schedule

8.2 Data Breach Policy

8.3 Acceptable Use of IT Facilities

8.4 Encryption Policy

8.5 Information Security Policy

VERSION:	**1.2**	**AUTHOR/ OWNER:**	**Office of the University Secretary**
Approved Date:	May 2018	**Approved By:**	Board of Governors
Review Date:	May 2019		