UNIVERSITY OF SOUTH WALES
PRIFYSGOL DE CYMRU

DATA PROTECTION POLICY

1. Introduction

The University needs to hold and process large amounts of personal data about its students, employees, applicants, alumni, contractors and other individuals in order to carry out its business and organisational functions.

As a data controller it is necessary for the University to ensure that it processes this data in accordance with the Data Protection Act 1998. Failure to do so could result in the institution being fined up to £500k.

Personal data is data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the University.

Some types of personal data can be more confidential than others, for example, details of a person's physical health or mental condition, and such data is known as sensitive personal data.

***** For clarification on terms and definitions please refer to the personal data Glossary and Definition Document.

2. Scope

This policy applies to all personal data held and processed by the University and its processors and would apply to:

- all employees of the University who are granted access to personal data;
- all contractors, suppliers, University partners and external collaborators and visitors who may be authorised to access University held personal data; and/or
- all locations from which personal data is accessed including home and off-site/ remote use.

3. Purpose

In accordance with the Data Protection Act 1998 the University has a number of obligations and as a data controller it must:

- To notify the Information Commissioner annually of the purposes for which it processes personal data
- To allow individuals to find out what information is held about them, the purposes for which the information is kept, where we obtain it from and to whom we might disclose it
- To process personal information in accordance with the 'Eight Principles of Data Processing' as set out in the legislation (below)

The policy is supported by specific guidance and procedures which have been developed to ensure staff and students comply with this legislation.

Principle 1 – Personal data shall be processed fairly and lawfully. The University must ensure that personal data is obtained fairly and that individuals, at the point of collection, are made aware how their information is to be used and to whom it will be disclosed.

For processing to be lawful, the institution must ensure that one of the following conditions are met (for sensitive personal data see further below).

- The data subject has given his/her consent to the processing
- The processing is necessary for the performance of a contract with the data subject, or for taking steps with a view towards entering into a contract
- The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract
- The processing is necessary in order to protect the vital interests of the data subject.
- The processing is necessary for the administration of justice; the exercise of functions under an enactment, the exercise of functions of the Crown or a government department; for the exercise of any other function of a public nature exercised in the public interest.

When processing sensitive personal data great care must be taken, and, in addition to the conditions above, processing will only be permitted if at least one of the following conditions is satisfied:

- The data subject has given their explicit consent.
- The processing is necessary for the purposes of performing any right or obligation imposed by law on the University in connection with employment.
- The processing is necessary to protect the vital interest of the data subject or another person.
- The information has been made public by the data subject.
- The processing is necessary for legal proceedings, obtaining legal advice or for the purposes of establishing, exercising or defending legal rights.
- The processing is necessary for the administration of justice; for the exercise of any functions conferred by or under any enactment; of for the exercise of any functions of the Crown or government department.
- The processing is necessary for medical purposes, and is carried out by a health professional or a person with an equivalent duty of confidentiality.
- The processing is necessary to trace equality of opportunity between people of different racial or ethnic backgrounds, different religious belief or different states of physical or mental health.

- The processing is in the substantial public interest; is necessary for the functions of a confidential counselling, advice, support or other service; and consent cannot be given by the data subject, the University of South Wales would not be expected to obtain the explicit consent of the data subject, or the processing must be carried out without their consent so as not to prejudice the provision of that counselling, advice, support or other service.
- The processing is in the substantial public interest and is necessary for research purposes; provide that the processing will not support measures or decisions with regard to individuals and will not cause substantial damage or distress to the data subject or any other person.

The University's fair processing notices advises individuals how their information will be processed.

Principle 2 – **Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**

Information obtained for a specified purpose is not to be used for a different purpose**.**

Principle 3 – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

The University will only collect the minimum amount of personal data required for the purposes required. Information is not to be collected on the premise that it might be useful in the future.

Principle 4 – Personal data shall be accurate and, where necessary, kept up to date.

The University will take reasonable steps to ensure the accuracy of personal data which it holds, and will take steps to amend, update or correct inaccurate data when requested to do so by the data subject.

Principle 5 – Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The University will ensure that personal information is not kept for longer than is required and staff must ensure that this information is securely destroyed once the purpose for processing has come to an end. University employees should refer to the 'Records Retention Schedule' for guidance on retention of data.

Principle 6 – Personal data shall be processed in accordance with the rights of data subjects.

When processing personal data the University will ensure that it is processed in accordance with the rights of data subjects:

- access to the information held about them by the University (through a subject access request);
- prevention of processing likely to cause damage or distress;
- prevention of processing for direct marketing;
- prevention of automated decision making;
- rectification, blocking, erasure and destruction of data;
- compensation for damage caused by illegal processing; and
- the right to request that the ICO carry out an assessment of personal data processing;

Principle 7 – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The University will take steps to ensure the security of personal data held both electronically and in manual form. Additional guidance is available on the data protection webpages and within the IT Regulations.

Principle 8 – Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The University will not transfer personal data outside the EEA unless the transfer is necessary and permitted in line with the Data Protection Act 1998.

4. Responsibilities

All staff and other approved users of University held personal data must be able to demonstrate competence in their understanding of data protection laws and good practice applicable to the performance of their University responsibilities. Staff must seek advice and guidance if they are unsure of how to process information or need any clarification.

When processing personal information staff must be do so in accordance with the procedures and guidance available.

Staff must undertake training when required.

University employees must report any actual or suspected breach in personal data security, “near misses” or working practices which jeopardise the security of personal data held by the University.

The University’s Information Compliance Manager is responsible for overseeing the University’s compliance with the Data Protection Act 1998 through advice, assistance guidance and the provision of training.

Non-compliance with this policy is subject to the University’s disciplinary procedures for staff and students.

Title: Data Protection Policy					
Version	**Issue Date**	**Revision Description**	**Author**	**Approved By & Date**	**Next Review Date**
1.0	Unknown	First Issue	Matthew Phillips	Unknown	Unknown
2.0	February 2016	Revision	Rhys Davies	VCEB February 2016	February 2018