**DATA PROTECTION APPROPRIATE POLICY - PROCESSING SPECIAL CATEGORY DATA AND CRIMINAL CONVICTIONS DATA**

1. **Introduction**

The University processes a range of personal data that relate to, prospective, current, former students/staff/research subjects.

This information is used for a number of purposes relating to day to day business, research purposes and management of the institution.

In addition to personal data the University also processes -

1. ‘special category’ personal data that includes the following types of information - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation.
2. Personal data relating to criminal convictions and offences.

Where sensitive data detailed in (i) and (ii) above is processed it is necessary for the University to have in place an appropriate policy document in place

1. **Purpose**

The purpose of this document is to ensure that the University complies with its obligations as outlined under Schedule 1, Part 4 of the Data Protection Act 2018 (DPA).

1. **Scope**

This document details the measures in place to ensure that the University will comply with the data protection principles when processing special category data and data about criminal convictions when it does so in reliance on a condition from Part 1, 2 or 3 of Schedule 1 of the DPA. It also explains our position in relation to retaining and erasing this type of personal data. It serves as an ‘appropriate policy document’ for the purposes of Part 4 of Schedule 1 DPA.

This document should be read in conjunction with the University’s ‘Data Protection Policy’ and ‘Privacy Notices’.

1. **Responsibilities**

This document applies to all employees, including temporary, casual, contract and agency staff, as well as any contractors or service providers acting on behalf of the University.

1. **Conditions from Article 9 of the General Data Protection Regulation**

Article 9 2(b) - Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment.

The University processes a variety of information about prospective, current and previous employees for employment purposes, including data about health and criminal convictions and associated proceedings. It is not appropriate to obtain consent for such processing due to the nature of the employer-employee relationship and because consent cannot be freely given or withdrawn; therefore the University relies on this condition for much of this processing. Personal data processed for employment purposes is treated confidentially and maintained by HR as part of applicant and employee personal files. It is only shared within the University on a strict need-to-know basis where the law allows. Where employees are seconded under contract to another organisation, or a secondee carries out work for the University, the University and the other organisation may share personal data in reliance on this condition, as set out in the applicable contract. Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements.

1. **Conditions from Schedule 1 DPA – Substantial Public Interest Conditions**

The University processes special category data and data about criminal convictions in reliance on the following conditions from Schedule 1 DPA. These are not the only legal bases/conditions on which we process special category data, but they are the only ones to which this document applies:

***Paragraph 6 – Statutory and Government purposes***

The University is legally required to provide some special category data about staff and students to external organisations for statutory returns and reporting, such as the data we provide to the Higher Education Statistics Agency (HESA). Only the minimum amount of data necessary to fulfil this requirement is provided and all data is shared securely.

We also rely on this condition to process data about students’ criminal convictions. This applies if a student is offered a place on a course which can result in employment in a regulated profession and the course involves an integral work placement which could not be undertaken if the student has a criminal conviction. We must process this data to ensure we do not admit a student onto a course which they cannot possibly complete. Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements.

To comply with its Tier 4 sponsor obligations the University must record engagement data relating to overseas students. Engagement with overseas students is monitored through biometric control. At enrolment overseas students on a Tier 4 visa have a fingerprint scanned which, through the use of an algorithm, is turned into a unique code. Information relating to the fingerprint is not retained and it is this unique code that is checked each time the student scans.

***Paragraph 8 – Equality of opportunity or treatment***

The University recognises the importance of equality of opportunity or treatment and monitors and reviews the existence or absence of this across all areas so that equality can be promoted and/or maintained. Any processing of the specified categories of personal data used for these purposes is carried out confidentially and securely. When it is collected as part of an application form, the data is stored separately from the rest of the application data.

***Paragraph 10 – Preventing or detecting unlawful acts***

We rely on this condition to process data about applicants’ and students’ criminal convictions, in certain circumstances, to enable us to manage any potential risks to the University community. Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements. We may also rely on this condition to process information about employees’ criminal convictions, if appropriate.

We also rely on this condition to disclose certain items of personal data to the police, DWP, or other similar bodies for the prevention and detection of unlawful acts. Any personal data disclosed under these circumstances is shared securely and only the minimum amount of information necessary is shared in any case.

The University has a duty to prevent individuals from being drawn into terrorism (known as the Prevent duty). Where we process special category data such as personal data about religious beliefs or political opinions, or data about criminal convictions, for the purposes of fulfilling our Prevent duty, we may rely on this condition where it is not appropriate to obtain an individual’s consent. Any personal data processed for these purposes is processed sensitively and confidentially on a strict need-to-know basis, in line with University and national Prevent procedures and guidance.

***Paragraph 11 – Protecting the public against dishonesty etc***.

The University runs many courses which lead to entry into a regulated profession or occupation. We may disclose special category data or data about criminal convictions to those who regulate such professions so that those regulators can exercise their functions appropriately by ensuring practitioners are fit and proper. There is a substantial public interest in enabling regulators to ensure that only those who are fit to practise a particular profession or occupation are able to do so.

***Paragraph 17 – Counselling etc.***

The University provides staff and student counselling services and a number of other student wellbeing services delivered by Student Services. The majority of special category data or data about criminal convictions is processed with the explicit consent of the individual using one of the counselling services; however if a circumstance arose which required us to process personal data without consent in order to provide confidential counselling, advice or support e.g. from Student Services, and such processing was in the substantial public interest, we would do so in reliance on this condition. All information held in counselling records is treated confidentially and stored securely and all counsellors comply with professional guidelines.

***Paragraph 18 – Safeguarding of children and of individuals at risk***

The University admits students who are under 18, as well as those over 18, to our courses and to our accommodation. We rely on this condition to process data about applicants’ and students’ criminal convictions, in certain circumstances, to enable us to identify and manage any potential risks to the University community. Any information about criminal convictions obtained as part of a Disclosure and Barring Service (DBS) check is stored and retained in line with DBS requirements. We may also rely on this condition to process information about employees’ criminal convictions, if appropriate.

1. **Data protection principles**

When processing personal data, anyone to whom this document applies will comply with the six data protection principles set out in Article 5 of the GDPR. The principles are summarised below, along with an explanation of how the University will comply with them whenever we process special category data or data about criminal convictions.

***Processed lawfully, fairly and in a transparent manner***

The data protection legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and in a transparent manner and without adversely affecting the rights of the data subject. In every case set out in Section 4, the data subject will be told who the controller is, the purposes for which the data are to be processed and the identities of any other parties to whom the data may be disclosed or transferred, among other things. This information will be provided to the data subject in a privacy notice at the time the data is collected, unless an exemption from the right to be informed applies in a particular case.

USW will process personal data lawfully by ensuring there is a legal basis for all the processing we undertake.

***Processed for limited purposes***

Personal data will only be processed for the specific purposes notified to the data subject via the privacy notice when the data was first collected or for any other purposes specifically permitted under the data protection legislation. Personal data will not be further processed in a manner which is incompatible with these purposes. This means that personal data will not be collected for one purpose and then used for an entirely different, unrelated purpose.

***Adequate, relevant and not excessive***

Personal data held about data subjects will be sufficient for the purposes for which it is held. Information which is not needed or is not relevant for a purpose will not be collected or otherwise processed. The minimum amount of personal data needed to properly achieve the purpose in question will be identified and collected; additional, excessive personal data will not be held.

***Accurate and up-to-date***

Personal data will be accurate and, where necessary, kept up-to- date. Information which is incorrect or misleading is not accurate; steps will be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

***Not kept for longer than is necessary***

Personal data will not be kept longer than is necessary for the purposes for which is it being processed. This means that data will be securely destroyed or erased from our systems when it is no longer required i.e. there is no legal requirement to retain it and there is no business or operational need for the information, taking account of the purposes for which it was originally requested.

***Will be kept securely***

The University will ensure that appropriate technical and organisational measures are taken to protect against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

1. **Non compliance**

If a person is concerned that the principles detailed within this document have not been followed in respect of personal data about themselves or others, that person should raise the matter with the Information Compliance Manager - dataprotection@southwales.ac.uk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version**  | **Issue Date**  | **Revision Description**  | **Author**  | **Next Review Date**  |
| 1.0  | March 2020 | First Issue  | Rhys Davies | March 2022 |
|  |  |  |  |  |