



Data Protection Policy

Key Messages

This document is a set of principles, rules, and guidance to be followed to ensure ongoing compliance with the UK GDPR (General Data Protection Regulation) and the Data Protection Act 2018.

This policy details the standards the University will follow and provides clarity in terms of the expectations of the institution in relation to the processing of personal data.

Who does this policy relate to?

This policy applies to all colleagues employed by the University of South Wales and Professional Support Services Ltd, as well as partners, contractors, consultants or other people who undertake paid or voluntary work on behalf of the University, or process personal data on behalf of USW Commercial Services Ltd, students who collect personal data relating to their studies as well as third parties who are given access to our documents, systems and/ or information processing facilities, hereafter referred to as 'colleagues' for the purposes of this policy.

This policy can be provided in hard copy upon request.

Table of Contents

Key Messages	1
Who does this policy relate to?	1
1 Introduction.....	3
2 Scope	3
3 Roles and Responsibilities.....	4

3.1 Controller.....	4
3.2 Data Protection Officer	4
3.3 Senior Information Risk Owner	4
3.4 Information Security Steering Group (ISSG).....	4
3.5 Deans and Departmental Directors	4
3.6 Data Protection Co-ordinators.....	4
3.7 Colleagues falling within the scope of this policy.....	5
4 Data Protection Principles and Individual Rights	6
4.1 The Principles.....	6
4.2 Data Subject Rights.....	7
5. Information covered by data protection legislation	8
5.1 Personal data	8
5.2 Pseudonymised and anonymised personal data.....	8
5.3 Personal data processing	9
6. Special category personal data	9
7 Fair and lawful processing	9
8 Data protection by design and default	10
9. International Data Transfers	10
10 Personal Data Sharing.....	11
11. Generative Artificial Intelligence (AI) Models	11
12. Direct Marketing.....	12
13. Data Protection and Information Security Training	12
14. Personal data breaches and incidents	13
15. Personal data security	13
15.1 Relevant policies and guidance.....	13
15.2 New systems or platforms	13
15.3 Hard copy personal data.....	14
15.4 Electronic personal data	14
15.5 Removable media	15
15.6 Verbal communications	15
15.7 Access to University systems	15
15.8 Destruction of personal data	16
15.9 Disclosure and transmission of personal data	16
15.10 Unlawful personal data processing.....	16

16. Records Management.....	17
17. Transparency	17
18. Governance and accountability	17
19. Consequences of non-compliance	18
20. Related Policies, Standards and Documentation	18
20.1 Policies.....	18
20.2 Regulations	18
20.3 Procedures.....	18
20.4 Guidance.....	18
21. Review	19
22. Document Control Information	19
23 Revision History	19
Appendix A.....	20

1 Introduction

To undertake its core functions and other services it is necessary for the University to collect, store, use and otherwise process personal data relating to individuals. The University takes the protection of all personal data seriously and is fully committed to the protection of the rights and freedoms of all individuals in relation to the processing of their personal data.

This policy provides a framework for ensuring that the University meets its obligations under the UK GDPR and the Data Protection Act (DPA) 2018.

This policy should be read and interpreted in conjunction with other related University of South Wales policies, regulations procedures and published guidance which provide appropriate direction on the application of the data protection legislation and are specified in Section 20 of this policy. A glossary of terms is included as Appendix A.

2 Scope

This policy applies to all colleagues employed by the University of South Wales and Professional Support Services Ltd, as well as partners, contractors, consultants or other people who undertake paid or voluntary work on behalf of the University, or process personal data on behalf of USW Commercial Services Ltd, students who collect personal data relating to their studies as well as third parties who are given access to our documents, systems and/ or information processing facilities, hereafter referred to as 'colleagues' for the purposes of this policy.

3 Roles and Responsibilities

3.1 Controller

As a controller of personal data, the University of South Wales is responsible for ensuring that appropriate measures are taken to ensure that personal data is processed in accordance with the data protection legislation and can demonstrate this.

3.2 Data Protection Officer

The University is legally required to appoint a Data Protection Officer {DPO} who is tasked with overseeing data protection compliance matters relating to the University of South Wales. This includes:

- Informing and advising the University of its obligations under data protection legislation
- Monitoring compliance with the regulations and related policies
- To advise on and monitor Data Protection Impact Assessments {DPIAs}
- Training and awareness raising
- Providing procedures, guidance, and advice in support of this policy
- Acting as the first point of contact and co-operate with the Information Commissioner's Office {ICO}
- Handling data subject rights requests
- Investigating personal data incidents and breaches

3.3 Senior Information Risk Owner

The Senior Information Risk Owner {SIRO} owns the overall risk arising from the processing personal data by the University. Our SIRO is the Chief Operating Officer.

3.4 Information Security Steering Group (ISSG).

ISSG is chaired by the SIRO. The group is responsible for the overview and scrutiny of information security and compliance arrangements

3.5 Deans and Departmental Directors

Deans and Directors are responsible for overseeing compliance with this policy and ensuring good data protection practice within their designated areas and maintaining an overview of activity within the faculty/department, identifying where 'Data Processing Agreements' {see Due Diligence Guidance} or 'Data Protection Impact Assessments' {see DPIA Guidance} may be required and seeking advice from the Information Compliance Team.

3.6 Data Protection Co-ordinators.

Within the current University structure, it is considered that the most effective means to ensure compliance throughout the institution is to have in place a Data Protection Co-ordinator{s} within each faculty/department. The co-ordinator will undertake the role of

liaison between the faculty/department and the Information Compliance Team. The co-ordinator role is a voluntary one to aid effective practice. Responsibility for processes and compliance remains within existing structures.

The Data Protection Co-ordinator will be responsible for the following:

- Being the faculty/departmental contact regarding data protection, information security and records management between the faculty/department and the Information Compliance Team (and vice versa) to raise issues and concerns.
- Promoting good practice in Data Governance and Records Management in their area.
- Attend Data Protection Co-ordinators Working Group meetings to raise issues around Data Governance and Records Management.
- Engaging with faculty/departmental line managers to provide updates on training compliance and remind managers of their responsibility to ensure colleagues complete the USW data protection and information security training modules

3.7 Colleagues falling within the scope of this policy

All colleagues as defined by Section 2 of this policy are responsible for:

1. Following this policy and any associated guidance and procedure
2. Ensuring the processing of personal data in any format is compatible with the data protection principles and that care is taken when handling personal data in any format. Personal data must be only processed (including viewed) where there is a legitimate business requirement and there is no conflict of interest.
3. Raising any concerns in respect of the processing of personal data with the DPO or Data Protection Coordinator
4. Promptly referring any requests made under the 'rights of the data subject' as set out in data protection legislation to the Information Compliance Team at dataprotection.southwales.ac.uk
5. Responding promptly to requests from the Information Compliance Team relating to point (4) above
6. Reporting personal data breaches and incidents immediately in accordance with the Data Incident Procedure and co-operating fully and promptly with the Information Compliance Team during their investigation into the incident
7. Successfully completing the University's data protection and information security training, including any refresher training
8. Attending any awareness raising sessions and taking note of any data protection communications issued on Connect

9. Completing Data Protection Impact Assessment Screening questions for all new projects, systems, software, and platforms that process personal data and submitting them to the Information Compliance Team in advance of any processing taking place
10. Completing full Data Protection Impact Assessments where a requirement has been identified and implementing any risk reducing measures as advised by the Data Protection Officer
11. Ensuring that third party suppliers are subject to the necessary due diligence checks before any processing begins
12. Ensuring that the personal data the University holds about them is accurate and up to date by informing the University of any changes or errors immediately
13. Ensuring that any third-party processing of personal data on behalf of the University is governed by a Data Processing Agreement {a legal requirement}
14. Where colleagues are sharing personal data with other organisations or any other third party, they must ensure that a legal basis allows the sharing to take place {and that this is documented} and that Information / Data Sharing Agreements are in place for any sharing that takes place on a regular basis
15. Students must adhere to data protection laws, this policy and any associated policies and guidance when processing personal data for purposes relating to their studies

4 Data Protection Principles and Individual Rights

4.1 The Principles

When processing personal data, the University is committed to complying with data protection legislation guided by the six data protection principles which state that personal data shall be:

- a) Processed lawfully, fairly and in a transparent manner;
- b) Used only for limited specified, stated purposes and not used or disclosed in any way 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;}
- c) Adequate, relevant, and limited to what is necessary to achieve the objective

- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that any personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay;
- e) 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 the appropriate technical and organisational measures required by the data protection legislation in order to safeguard the rights and freedoms of individuals;
- f) 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, using appropriate technical or organisational measures.

In addition, the accountability principle requires the University to be able to evidence that its processing complies with these six principles. To meet these obligations, the University has appropriate measures and records in place to be able to demonstrate compliance and our processing is documented within our Records of Processing Activities (ROPA). The University makes its Appropriate Policy Document available which outlines how it processes special categories of personal data and criminal offence data.

4.2 Data Subject Rights

The University will ensure that personal data will be processed in line with the rights of the individual:

- a) The right to be informed - Individuals will be advised how their personal data is to be used.
- b) The right of access - Individuals will have a right, upon request, to obtain a copy of their data.
- c) The right to rectification - Where appropriate, individuals are entitled to have inaccurate data rectified.
- d) The right to erasure - Individuals are able to request that personal data is erased.
- e) The right to restrict processing - Individuals may suppress processing where appropriate.

- f) The right to data portability – Individuals may request for their information to be moved from one IT (Information Technology) environment to another without hindrance to usability.
- g) The right to object – Individuals are able to object to processing in prescribed situations.
- h) Rights in relation to automated decision making and profiling – where decision making is made automatically individuals can object to their data being processed in this manner.

The University has a statutory 28 days to comply with a request to exercise any of these rights - from the time that the request is received by any staff member within the University. If any colleague receives such a request, it must be referred to the Information Compliance Team without delay. We have dedicated resource and clear processes to handle subject access requests and other information rights requests.

5. Information covered by data protection legislation

5.1 Personal data

The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person and is further defined at Appendix A of this policy

5.2 Pseudonymised and anonymised personal data

Pseudonymised personal data is captured by the legislation, however anonymised data is not. Anonymised means that individuals are not identifiable and cannot be re-identified by any means likely to be used. Data protection law does not require anonymisation to be completely risk-free. Colleagues must be able to mitigate the risk of re-identification until it is sufficiently remote that the information is 'effectively anonymised.'

Anonymisation processes should consider the concept of identifiability in its broadest sense and should not simply focus on removing obvious information that clearly relates to someone. The removal of direct identifiers such as a name or identification number is insufficient to ensure effective anonymisation.

If the University can identify an individual by combining information with other information it holds, the information is pseudonymous, not anonymous and the data

protection legislation must be complied with.

5.3 Personal data processing

The legislation applies to all personal data processing. Processing is anything you do with data during its lifecycle, from the point of collection right up to destruction. The definition of processing is set out at Appendix A.

Colleagues must comply with this policy and associated policies even when simply viewing or verbally disclosing personal data - this is processing and is captured by the data protection legislation. Personal data must only be processed where there is a legitimate business requirement. If you are legitimately required to access or update a record of a person known to you personally, ensure that you bring it to the attention of your line manager prior to accessing the record. Line managers must consider whether there is a conflict of interest and whether the access would be unfair to the data subject. If so, another colleague should be tasked with carrying out the work.

6. Special category personal data

The data protection legislation defines special category data as:

1. Race or ethnic origin;
2. Political opinions;
3. Religious or philosophical beliefs;
4. Trade union membership;
5. Genetic data;
6. Biometric ID data;
7. Health data;
8. Sexual life and/or sexual orientation; and
9. Criminal data {convictions and offences}

This type of information will be subject to additional protection. Most processing involving this type of data will require a Data Protection Impact Assessment {DPIA} as described in Section 8 of this policy and colleagues will ensure that an Article 9 lawful basis applies {see Appendix A}

7 Fair and lawful processing

The University collects personal data during the application process, enrolment,

recruitment, provision of services to service users together with other purposes relating to its functions including research.

To ensure that personal data is processed fairly, there is a requirement to ensure that individuals are made aware of how the University will use their data. Individuals will be provided or directed to with a privacy notice covering those particular purposes at the point of the personal data collected (if collected directly from the data subject).

Where personal data is obtained from other sources, the University will provide the individual with information relating to the processing within one month of obtaining the data unless an exemption applies.

For personal information to be processed, there must be a lawful basis for the processing. The lawful conditions are set out in Appendix A.

8 Data protection by design and default

Data protection will be embedded into processing activities right from the start. Privacy considerations must be undertaken from the outset, not as an afterthought.

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project or processing activity.

The University is legally required to conduct a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing:

- Systematic and extensive profiling with significant effects
- Special category or criminal offence data on a large scale
- Systematically monitor publicly accessible places on a large scale

In addition to this legal requirement, the University will conduct a DPIA for any project or processing which may result in a risk to individuals.

DPIAs must be subject to regular review by the process owner in conjunction with the Data Protection Officer.

If a pre-existing high-risk processing activity has not been subject to a DPIA, one will be conducted as a priority.

9. International Data Transfers

The University will not transfer personal data to a receiver located in a country outside the UK unless there are approved appropriate safeguards in place.

Colleagues must seek advice from the Information Compliance or Legal Team before transferring or making any personal data available to a separate legal entity located outside the UK. This includes staff names and email addresses.

The University will map its flows of international personal data.

10 Personal Data Sharing

Before personal data held by the University can be shared with a third party such as another University or external stakeholder, the University will have to review or put in place an arrangement to ensure that the sharing is lawful in line with data protection laws. Where sharing is necessary on a one-off basis then an agreement is not required, and sharing can proceed provided a lawful basis is in place and the data protection principles are complied with. However, where the sharing is going to be part of an ongoing arrangement such as a research project or as part of a funding requirement the University it is essential that an Information Sharing Agreement is put in place.

In the event that the University engages a third party to process personal data on its behalf, a specific written contract with the third-party providing assurance in respect of the management of the data and containing clauses as set out in Article 28 of the UK GDPR must be in place – this is a legal requirement.

There is no requirement for an Information Sharing Agreement or a contract when sharing personal data internally within the University, provided that a lawful basis is met, and the principles are complied with. Colleagues must consider whether it is necessary to share each piece of personal information and whether they could achieve the same outcome by sharing less.

11. Generative Artificial Intelligence (AI) Models

11.1 Entering personal data into a generative AI model

Any data entered into a publicly available generative AI model could effectively be a third party disclosure (depending on the model). The provider could use this data to train the model or share it with other parties which presents significant security and privacy concerns. Data subjects may not know that their data is being used for this purpose and they may not be able to exercise their rights. There may not be a legal basis for the processing.

Colleagues must not enter any personal data controlled or processed by the University, into any generative AI model, (including but not limited to Chat GPT) unless a Data Protection Impact Assessment (DPIA) has been conducted on the platform and the processing approved by IT Security and Compliance.

Colleagues must remind themselves of the definition of personal data. Remember that it may be possible to identify someone from the data, even when a name is not included. It may be possible for the model to identify an individual by combining the data with data it already holds.

11.2 Using generative AI to make decisions about individuals

Colleagues are also prohibited from using any generative AI platform to make a judgement or a decision about an individual unless a DPIA has been carried out as well as all consultation, approval and escalation requirements met.

Generative AI models cannot be relied upon to produce accurate results and therefore any decision-making process could be flawed which may lead to an unfair outcome for an individual.

Individuals have the right to not be subject to a decision based solely on automated processing which produces legal effects or significantly affects him or her.

Colleagues should refer to the University [Generative AI Guidance](#) on the CELT Hub.

12. Direct Marketing

The University in the course of its work may wish to use personal data for purposes relating to marketing activities. Colleagues must adhere to the Privacy and Electronic Communications Regulation (PECR), the UK GDPR and the Data Protection Act 2018 when engaging in direct marketing activity and will follow the University's Data Protection and Marketing Guide.

13. Data Protection and Information Security Training

All colleagues who process personal data and / or have a University IT account are required to complete the University's Data Protection and Information Security training. Training must be completed before the colleague processes any personal data held by the University and no later than two weeks after the colleague's start date.

Thereafter, all colleagues handling personal data are required to complete the University's mandatory refresher training at least every two years.

Colleagues may also be required to undertake additional training or attend awareness sessions as and when the need arises.

The University will maintain a record of all individuals who have completed and passed the training in order that it can demonstrate compliance with its data

protection obligations. Where colleagues fail to complete the training within the specified time a notification will be sent to the line manager and an escalation process will be followed prior to referring the colleague to the HR (Human Resources) Advisor in accordance with the conduct procedures. The Data Protection Co-ordinators will also have some involvement in reminding colleagues to complete the training.

Failure to complete the mandatory training within these time limits would constitute a breach of this policy and may result in disciplinary action.

We have a clear communication plan which seeks to embed a culture of privacy and risk orientation.

14. Personal data breaches and incidents

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes personal data in all formats, whether electronic, hard copy, or information disclosed verbally. Where a breach is identified, colleagues must report it in line with the Data Incident Procedure immediately after becoming aware of the breach.

Any incident or 'near miss' that threatens the security of personal data shall also be reported without undue delay in accordance with the Data Incident Procedure. When incidents go unreported, they cannot be addressed and could later develop into a serious issue for the University.

15. Personal data security

15.1 Relevant policies and guidance

Colleagues must ensure that personal data in all formats, including but not limited to electronic and hard copy are managed securely. Colleagues must comply with IT Security policies and regulations and Information Compliance policies and guidance when handling personal data. The relevant policies and guidance can be found on the IT and University Secretary's intranet pages at Section 20 of this policy.

15.2 New systems or platforms

Where colleagues are considering using a new system, platform or web application which will collect, store, or otherwise process personal information, colleagues must raise a call with IT Services and the supplier must complete the relevant questionnaires as outlined in Section 11 of this policy. The University's Due Diligence Guidance must

be considered.

15.3 Hard copy personal data

The storage of hard copy personal data within desks and cupboards should be avoided unless there is a legal requirement and/or there are stringent physical security measures in place, in line with the Information Classification Policy.

Offices or rooms containing personal data must be locked when empty or not in use and desks, cupboards and filing cabinets must be kept locked if they contain personal data. Special category or sensitive data must be stored using two separate locks (i.e., a locked cabinet within a locked room). Ensure any documents containing personal data are not left exposed in accordance with the Clear Screen and Clear Desk Policy.

When colleagues vacate rooms or close IT systems there is a need to ensure that steps are taken to protect personal data and to ensure that it is kept in a way that is accessible to authorised colleagues and in line with the Records Retention and Protection Policy.

15.4 Electronic personal data

Monitors must be positioned in suitable locations to ensure that confidential personal data is not visible to passers-by or other unauthorised individuals e.g., through office windows or doors. Users must lock their PCs and other devices before leaving them unattended to prevent unauthorised access to systems in accordance with the Clear Desk and Clear Screen Policy. Colleagues must not allow anyone access to their IT account or share their password in accordance with the University's IT Computing Regulations.

The University's Information Classification Policy contains details of the restrictions and practices required to protect information being stored and processed on mobile devices. These restrictions and practices depend on the classification of the information and must be followed.

Any person who has access to a University owned device or access University systems via a personally owned mobile device must abide by the University's Mobile Device Policy to mitigate the risk of loss or theft of data, compromise of classified information and the introduction of viruses and malware.

Personal data classified as 'Private' or 'Confidential' as defined in the Information Management / Classification Policy must not be stored on a personally owned device.

Personal email accounts must not be used for University business. Only University accounts can be used for these purposes.

Colleagues must be aware that their University owned device will be monitored in accordance with the Logging and Monitoring Policy.

15.5 Removable media

Removable media includes but is not limited to USB flash drives, floppy disks, CD ROMs, and tapes.

Colleagues should avoid storing personal data on removable media unless there is a specific business requirement and password protection / suitable encryption is used. Items must be wiped when no longer in use.

15.6 Verbal communications

Colleagues must understand the importance of maintaining confidentiality of verbal conversations. All verbal communications, including discussions, meetings, and phone calls where specific individuals are the subject, should be treated as Private or Confidential unless otherwise known or stated.

Verbal conversations about a specific individual must not be overheard, recorded, or disclosed without authorisation and / or a lawful basis.

The University will implement reasonable measures to ensure that verbal conversations are not overheard in public areas, meeting rooms and offices. This includes maintaining secure and private meetings spaces and soundproofing, as necessary.

15.7 Access to University systems

When a colleague is ceasing employment or a student contract expires, they must not retain any University owned personal data unless by an explicit written transfer agreement consistent with the data protection principles. The HR leavers checklist must be followed.

When a colleague is transferring to a different department or role, action must be taken to revoke access to any sites, shared drives, platforms, or systems that are no longer required. This is the responsibility of the relevant line manager. Any departmental personal data held in any other location must be returned or deleted before the transfer unless there is a legitimate business requirement to retain.

Any person requesting access to their IT account following the end of an employment contract must seek approval from IT Services and Compliance. The relevant business area will be consulted with, and a risk assessment will be conducted. Approval will not be granted unless there is a strong justification.

15.8 Destruction of personal data

Personal data must be destroyed in accordance with the Record Retention Schedule. Early deletion could constitute a data breach.

Paper documents containing personal data must be disposed of securely via the University's confidential waste service.

Removable media items such as USB sticks, CDs must be wiped or destroyed securely to ensure that the information is no longer accessible. Equipment such as laptops, PCs, smartphones must be wiped and/or disposed of securely in accordance with the University's Disposal of Confidential Waste & ICT (Information and Communications Technology) Equipment Policies and Procedures.

15.9 Disclosure and transmission of personal data

Personal data must not be disclosed to unauthorised third parties intentionally or through negligent actions. Personal data must not be disclosed (in writing or verbally) to third parties unless it has been verified that the recipient has the authority to access that information and a lawful basis has been identified.

Colleagues must use the most secure method of transmission. The most secure way to share information is via SharePoint or Teams, ensuring that access is only granted to the intended recipient. Any link must be carefully shared.

Post is a secure method of transmission. Always ensure that the envelope is sturdy and securely sealed. It may be necessary to use recorded or tracked delivery in cases where sensitive information is contained in the correspondence and where distress would be suffered by a data subject in the event of an item of post going missing.

If the recipient is unable to receive information via SharePoint or Teams and post is not possible or practical, you can send personal information via email if you follow the Information Management / Classification Policy and the University Email Guidance.

15.10 Unlawful personal data processing

Unlawful processing of personal data would include (but not limited to) accessing, personal data for private interest or disclosing, altering, or destroying personal data for personal gain. Deliberate or reckless unlawful processing of personal information is a criminal offence for which individuals could be prosecuted.

Any colleague found to have engaged in unlawful processing will be subject to disciplinary proceedings which could result in dismissal.

16. Records Management

Personal data held about individuals must be adequate and relevant for the purposes for which it is held. The minimum amount of personal data needed should be identified and collected.

Colleagues will ensure that personal data is accurate and where necessary, kept up to date. The accuracy of personal data should be checked regularly, and individuals must have a means of updating their information when required.

The University will only keep personal data for as long as is necessary in accordance with retention schedules maintained by the University, information identified for destruction must be erased or disposed of securely.

17. Transparency

Transparency is fundamentally linked to fairness. Approved University assets and channels must be used for processing personal data on behalf of the institution.

It is not permitted to use any personal social media platform, personal email, or text messaging to discuss or make decisions in relation to individuals from a business perspective. Please refer to the Social Media Policy. Such processing results in the creation of unmanageable records and creates risk to the security of such information.

Personal data will only be processed for the specific purposes notified to the individual via the privacy/fair processing notice when the data was first collected or for any other purposes specifically permitted under data protection legislation. Personal data must not be collected for one purpose and then used for an entirely different, unrelated purpose. Where it is necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs, unless an exemption from this requirement applies.

18. Governance and accountability

The University will appoint a Data Protection Officer (DPO) who will have a direct line to the Vice-Chancellor and a regular report will be presented to a formal meeting of the Information Security Steering Group (ISSG), the Audit Committee and the Board of Governors.

Colleagues or students wishing to make a complaint may do so through the 'Complaints Procedure'.

19. Consequences of non-compliance

Failure to comply with this policy may result in disciplinary action in line with the University's policies and procedures.

Suppliers, contractors, partners, students or anyone undertaking paid or unpaid work on behalf of the University are asked to comply with the policy in so far as it is applicable to their activities. Compliance will be discussed in contract management meetings and non-compliance will be considered against contractual obligations.

20. Related Policies, Standards and Documentation

20.1 Policies

[Information Management Policy](#)

[Information Classification Policy](#)

[Information Security Policy](#)

[Records Retention and Protection Policy](#)

[Clear Desk and Clear Screen Policy](#)

[Social Media Policy](#)

[Logging and Monitoring Policy](#)

[Mobile Device Policy](#)

[University's Disposal of Confidential Waste & ICT Equipment Policy and Procedures](#)

[Appropriate Policy Document](#)

20.2 Regulations

[IT Computing Regulations](#)

20.3 Procedures

[Data Incident Procedure](#)

[Complaints Procedure](#)

20.4 Guidance

[Disclosing student personal information to third parties Guidance](#)

[Data Protection and Marketing Guide](#)

[Due Diligence Guidance](#)

[DPIA Guidance](#)

[Data Sharing Agreements I University of South Wales Guidance](#)

[Email Guidance](#)

[Generative AI Guidance](#)

[Records Retention Schedule](#)

21. Review

This policy will be reviewed every two years.

22. Document Control Information

Policy Author	Eloise Rosser, Data Protection Officer and Information Compliance Manager, University Secretary's Office
Information Classification	Public
Version	2.0
Status	Published
Approval Body	Information Security Steering Group (ISSG)
Effective Date	26/02/24
Equality Impact Assessment completion date	23/10/23
Review Date	12/02/26

23 Revision History

Version	Date of Review	Description of changes	Approved By & Date
2.0	12/02/24	Re-write	Information Security Steering Group 12/2/24

This is a controlled document and is only considered valid when viewed via the University of South Wales Intranet or external website. If in hard copy or saved to another location, it is the individual's responsibility to check the version number matches the Intranet. Approved policies are valid from the effective date and until an updated version has been uploaded to the Intranet.

Appendix A

Definitions

Automated Decision-Making - Automated decision-making takes place where decisions are made solely by automated means without any human involvement.

Controller - means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

Data Protection Legislation - means the UK GDPR and the Data Protection Act 2018

Data Subject - is the individual who is the subject of personal data.

Personal Data - means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, id number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identify of that natural person.

Processing - means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction

Processor - means a natural or legal person, public authority, agency, or any other body which processes personal data on behalf of the controller (*not including agents/ employees of the controller*)

Profiling - Profiling means automated processing of personal data to evaluate certain things about a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, reliability, behaviour, or movements.

Special Category Personal Data is personal data relating to ethnic origin, political opinions,

religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures.

Lawful bases

Lawful bases for processing general personal data (defined in Article 6 of the UK GDPR):

- (a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) **Legal obligation:** the processing is necessary for you to comply with the law {not including contractual obligations}.
- (d) **Vital interests:** the processing is necessary to protect someone's life.
- (e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. {This cannot apply if you are a public authority processing data to perform your official tasks.}

Lawful bases for processing special category personal data (defined in Article 9 of the UK GDPR)

- {a) Explicit consent
- {b) Employment, social security, and social protection {if authorised by law}
- {c) Vital interests
- {d) Not-for-profit bodies
- {e) Made public by the data subject
- {f) Legal claims or judicial acts
- {g) Reasons of substantial public interest {with a basis in law}
- {h) Health or social care {with a basis in law}
- {i) Public health {with a basis in law}
- {j) Archiving, research, and statistics {with a basis in law}

