Information Management Policy

Key messages

This policy outlines the University's approach to information management at a high-level.

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.

A hard copy version of this policy can be provided on request and is available in Welsh.

Contents

1 Introduction

1.1. This policy sets out our commitment to following our guidelines and procedures and is designed to promote the effective management of information at the University.

1.2 This policy together with associated polices, guidance and procedures applies to the management of all information, in both digital and physical formats, created or received by the University.

1.4. Our information is a valuable corporate asset, and our records provide evidence of what we do and why. We know what information we hold, why we hold it, and we manage information according to its sensitivity. We create and manage records efficiently, make them accessible where possible and we protect and store them securely.

1.6. By adopting this policy, we aim to ensure that information, whatever form it takes, is accurate, reliable, ordered, complete, useful, up to date and accessible whenever it is needed to help us:

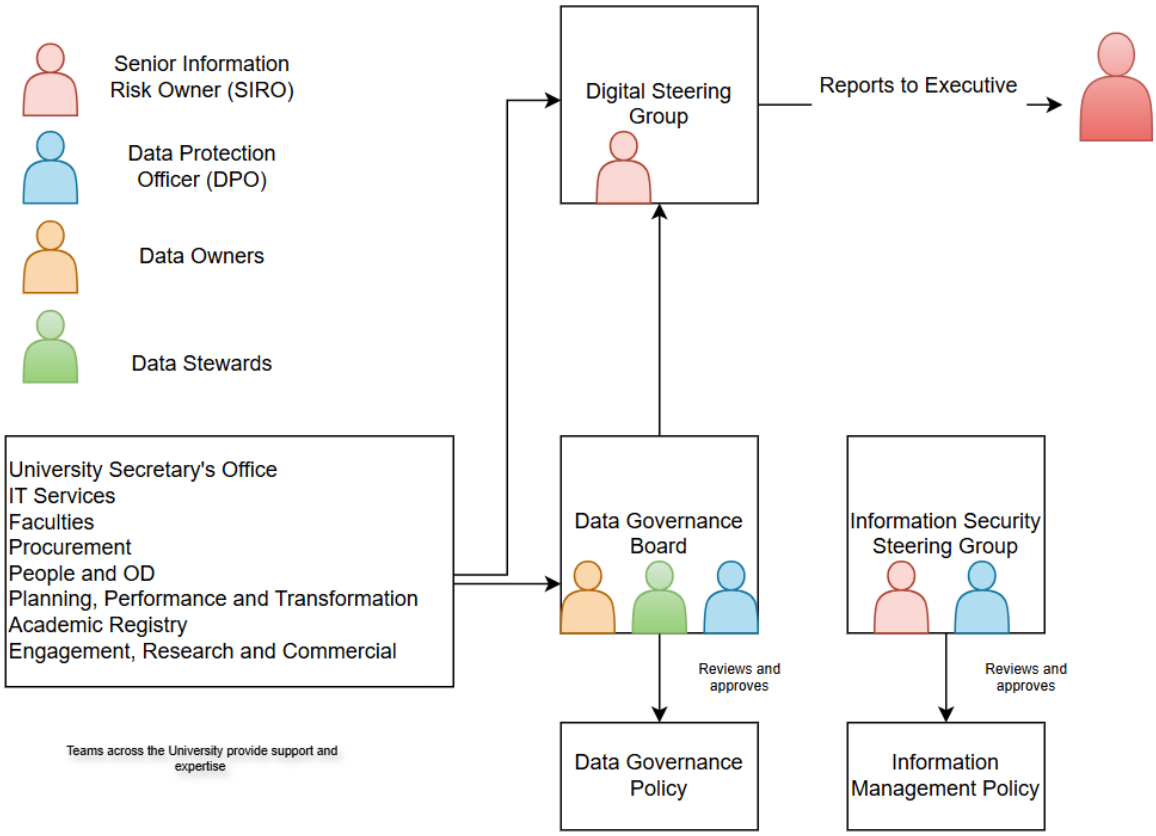
- carry out our business
- make informed decisions
- provide an audit trail to meet business, regulatory and legal requirements and;
- protect the rights of our employees and our students.

2. Statutory Framework

2.1. This policy provides a framework for meeting our responsibilities under relevant legislation, guidance and codes of practice including the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)
- Freedom of Information Act 2000
- Environmental Information Regulations 2005
- Section 46 Code of Practice on the management of records
- Information Commissioner's Code of Conduct

3. Roles and Responsibilities



3.1. All colleagues have a responsibility to ensure the University manages its information and any associated risks appropriately and in accordance with this policy and its associated guidance and procedures.

3.2. To ensure that responsibility for delivering good standards of information management practice is embedded throughout the organisation we have assigned specific roles to individual staff. In summary, these roles are as follows:

Data Protection Officer (DPO) - As a public authority, the University is legally required to appoint a DPO. The DPO is responsible for monitoring internal compliance, informing and advising the University on its data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting as a contact point for data subjects and the Information Commissioner's Office (ICO). The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

Senior Information Risk Owner (SIRO) - The SIRO holds executive responsibility for managing information risk and chairs the Information Security Steering Group. This role includes oversight of the University's data protection and information security framework and ensuring that information risk

management aligns with and supports the University's strategic objectives. The SIRO also provides assurance to the Executive team that information risks are being effectively identified and managed. Additionally, the SIRO is accountable for making formal decisions on the acceptance of specific information risks.

Data Owners - role and responsibilities are set out in the Data Governance Policy.

Data Stewards – role and responsibilities are set out in the Data Governance Policy.

3.3. Our SIRO is the member of Executive nominated by the Vice Chancellor, (normally Chief Operating Officer or equivalent) and our DPO is the Information Compliance Manager.

3.4 The Information Security Steering Group (ISSG) chaired by the SIRO is concerned with ensuring that risk to information security is appropriately managed.

3.5 The University has an ISSG Charter which presents the philosophy of information security within the University and represents the endorsement of the University executive management team.

3.6 The Data Governance Group ensures effective oversight of data governance and aims to extend a data governance programme across the University. The Data Governance Policy clarifies the roles and responsibilities of executive sponsors or nominees, data owners, and data stewards.

3.7 The Digital Steering Group provides oversight of the digital direction for the University and leadership in co-ordinating and prioritising digital strategy deliverables and makes key strategic decisions relating to the performance and delivery of the digital portfolio activities.

3.8 Central support to the Information Security Steering Group, Data Governance Committee and the Digital Steering Group is provided by several teams at the University with responsibilities and appropriate skills to deliver the following functions: Information Compliance, Information Security, IT Services, Academic Registry, Governance, Faculties, Legal , Procurement, People and Organisational Development, Faculties, Student Life and Planning, Performance and Transformation.

3.9. The Head of Compliance leads the Information Compliance team. This team is responsible for advising the University on information compliance matters, ensuring that the university meets its statutory requirements under data protection legislation and associated guidance and also for producing policies, procedures and guidance relating to the management of information.

4. Managing Risk to Information

4.1. ISSG, provides overview and scrutiny of information compliance and security arrangements and considers escalated issues for decisions.

4.2 The Senior Information Risk Owner (SIRO) holds Strategic and Operational responsibility for Risk. The Planning Manager is responsible for the day-to-day management and co-ordination of risk on behalf of the SIRO.

5. Protection of Personal Data

5.1. The University's Data Protection Policy provides a framework for ensuring that the University meets its obligations under the UK GDPR and the DPA 2018. It applies to all the processing of personal data carried out by the University including processing carried out by partners, contractors, consultants and processors.

6. Storage of Information at the University

6.1. We must store our information in locations, appropriate to its format, content and sensitivity. We ensure appropriate controls are in place to maintain the confidentiality, integrity and availability of our information. Our Information Classification Policy provides instruction on appropriate storage locations.

7. Information Security

7.1. We ensure the security of our information via the implementation of a number of policies, procedures and guidance. Our Information Security Policy supported by our Information Classification Policy ensures that information within our care receives an appropriate level of protection according to its sensitivity and criticality. Colleagues use University systems in line with our IT Computing Regulations, Information Classification Policy, Information Security Policy and policies within our Information Security Management System (ISMS) and our Clear Screen and Clear Desk Policy.

8. Retention and Disposal

8.1. Our Record Retention and Protection Policy outlines our approach to managing the retention and protection of our records. It provides for a consistent approach and applies to all physical and digital records, regardless of storage location.

8.2 Our Disposal of Confidential Material Policy (sits under our Disposal of Confidential Waste and ICT Equipment Policies and Procedures) covers the disposal of material containing personal information or information that is considered to be confidential. This policy sets out the process that must be followed when destroying or disposing of electronic media and paper based records.

8.3 The University's Record Retention Schedule is a document that sets out the classes of records the University holds and details the period they need to be kept for. The schedule is based on the

content of the document rather than its format and applies to electronic and paper records. University functions and keywords can be searched within the document. The University has a separate Retention Schedule for Student Recruitment.

8.4 Our retention periods are driven by legislation, regulatory or business need and are based on the JISC retention periods. If there is no existing defined retention period for the information, it is the responsibility of the relevant data owner (with input from the Information Compliance Team) to determine an appropriate retention period.

9. Additional Policies and Training

9.1 This policy is supported by the following Information Compliance and IT policies

- Data Protection Policy
- Data Governance Policy
- Information Classification Policy
- Information Security Policy
- Records Retention and Protection Policy
- IT Computing Regulations
- Disposal of Confidential Waste & ICT Equipment Policy and Procedures
- Clear Screen and Clear Desk Policy

9.2 Additional policy, procedure and guidance documents providing more detailed and subject-specific information to further its objectives are available to colleagues on the University Intranet site.

9.3 This policy is also supported by training e.g. the University's Data Protection and Information Security training packages and awareness sessions.

10. Review

10.1 This policy will be reviewed every two years

11. Document Control Information

Policy Author	Eloise Rosser, Data Protection Officer and Information Compliance Manager, University

	Secretary's Office
Information Classification	Public
Version	Published
Approval Body	Information Security Steering Group (ISSG)
Effective Date	26/02/24
Equality Impact Assessment completion date	23/10/23
Review Date	26/02/26

12. Version History

Version	Changes made	Date published	Made by
4.0	Re-write	26/02/24	Eloise Rosser, Data Protection Officer
4.1	Clarification of roles and responsibilities and amendments following restructure. Updated 6.1 to reflect responsibilities for risk management and co-ordination.		Eloise Rosser, Data Protection Officer
4.2	Updates following restructure and changes to Executive / SIRO. Minor amendments to wording.	09/06/26	Eloise Rosser, Data Protection Officer

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.