INFORMATION SECURITY POLICY			
Department	ICT Services		
Author	Legal Services Advisor		
Authorised By:	Director of Operations		
Implementation By:	Associate Director for IT Services		
Policy Reference:	POIT1718009		
Policy Replaced:	NA		
Version No:	1	**Approval Committee:**	VCB
Date approved:	17.04.18	**Minute no:**	17.96.03
Status:	Approved	**Implementation Date:**	May 18
Period of approval:	3 years	**Review Date:**	May 21
I have carried out an equality impact assessment screening to help safeguard against discrimination and promote equality.			✓
I have considered the impact of the Policy on the Welsh language and Welsh language provision within the University.			✓

1. PURPOSE AND SCOPE

1.1 The purpose of this policy is to set out the University's approach to information security management. Information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as WGU, where information will relate to learning and teaching, research, administration, management and business operations.

1.2 The documents in the Information Security Policy Framework in Appendix 1 apply to all information assets which are owned by the University, used by the University for business purposes or which are connected to any networks managed by the University. The documents in the Information Security Policy set apply to all information which the University processes, irrespective of ownership or form. The documents in the Information Security Policy set apply to all members of the University and any others who may process information on behalf of the University. This policy is owned, managed and developed by the Associate Director for IT on behalf of the University.

1.3 The scope of the Information Security Policy is concerned with the management and security of the University's information assets (an information asset is defined to be an item or body of information, an information storage system or an information

processing system which is of value to the University) and the use made of these assets by its members and others who may legitimately process University information on behalf of the University.

1.4 This policy and the Framework applies to:

- Anyone within Glyndŵr University who accesses University information assets or technology. This includes users[1], students and alumni.
- Technologies or services used to access or process University Information assets
- Information assets processed in relation to any University activity or function, including by, for, or with, external parties
- Information assets that are stored by the University or an external service provider on behalf of the University
- Information that is transferred from and/or to the University for a functional purpose
- 3rd party, public civic or other information that the University is storing, curating or using on behalf of another party
- Internal and/or external processes that are used to process, transfer or store University information

1.5 This Policy and the Framework are designed to:

- Promote a holistic approach to information security management
- Protect the University's information and technology against compromise of confidentiality, integrity (including non-repudiation[2]) and availability.
- Support the University's strategic vision through an approach which effectively balances usability and security
- Facilitate a 'security aware' culture across the University and promote that Information Security is everyone's responsibility
- Protect the University's information assets, and 3rd party data assets being processed or held by the University on behalf of another party, and technology by identifying, managing and mitigating information security threats and risks
- Assist in the compliance of contractual, legal or regulatory obligations
- Identify, contain remediate and investigate information security incidents to maintain and assist in improving the University information security posture
- Ensure that the University is compliant with its information security obligations, especially those related to the hosting, curation or processing of 3rd party data

[1] Users are defined as all staff, contractors, visitors, consultants and 3rd parties engaged to support the University activities and functions (including Governors) and who have any authorised access to any University information assets.

[2] Non-repudiation implies that in a transaction one party cannot deny having received a transaction nor can the other party deny having initiated it. It is often included within integrity but is expanded here for completeness

- Provide assurance to other parties that we have a robust control environment in place to protect their data through an effective information security management system

2. RELATIONSHIP WITH EXISTING POLICIES

This policy and the Policy Framework set out in **Appendix 1** advocates a holistic approach to information security and risk. This is achieved by identifying and assessing Information Security threats and developing and implementing a combination of people, processes and technology controls to mitigate information security risks according to the University's defined level of risk and the desired objectives.

3. POLICY STATEMENT

WGU is committed to preserving the confidentiality, integrity and availability of all its key information assets in order to assure legal and contractual compliance and reputation. The information security framework outlined in **Appendix 1** will encompass this policy, supporting policies, processes and tools and the requisite management and decision-making structures) shall be an enabling mechanism for information sharing and for reducing information-related risk to acceptable levels.

Information Assets are identified, classified and protected in accordance with the above stated policies and processes and tools. Any security controls which are implemented must be proportionate to the defined classification. Key information assets are governed by an appointed data protection officer in accordance with the key responsibilities defined in the Data Protection Officer Role document on http://www.glyndwr.ac.uk/data-protection/DPO

The Policy is in place to support the strategic vision of the University and to facilitate the protection of the University's information and technology services against compromise of its confidentially, integrity and availability. Whilst doing this, it recognises the ability to discover, develop and share knowledge must be maintained

Members of staff and any other individuals within scope outlined in 1.4 of this Policy must:

(i) Complete the Information Security Awareness Training

(ii) Ensure that reasonable effort is made to protect the University's information and technology from accidental or unauthorised disclosure, modification or destruction

Please see the Framework in Appendix 1 for the Policies relevant in order to comply with (i) and (ii) above. Where the University enters into arrangements or partnerships with other Universities outside of the EU, we need to ensure that the agreements or arrangements have appropriate mechanisms in place to comply with (ii) above.

4. INFORMATION SECURITY PRINCIPLES AND OBJECTIVES

4.1 The University has adopted the following principles to underpin this policy;

1. Information will be protected in line with all relevant University policies as outlined **in Appendix 1** and legislation, notably those relating to data protection, human rights and freedom of information, and in line with all legal and statutory requirements as may be current at the time.

2. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.

3. Information will be processed according to a clearly defined and agreed purpose, made available solely to those who have a legitimate need for access, and retained in accordance with the appropriate guidance

4. All information will be classified according to an appropriate level of security.

5. The integrity of information will be maintained.

6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.

7. Information will be protected against unauthorised access.

8. Compliance with the Information Security policy will be enforced.

4.2 Information Security Objectives

4.2.1 The University will manage the risks it faces in relation to information security, keeping its risk exposure to acceptable levels as defined by the University's risk appetite. The governance structure shall include allocation of ownership of information security risks and information assets to provide accountability, and the establishment of risk assessment policy and processes.

4.2.2 The risk assessment method shall provide a consistent and systematic approach to estimating the magnitude of risks and the process of comparing the estimated risks against risk acceptance criteria to determine the significance of the risks and any changes to risk over time.

4.2.3 The Policy will create consistency of approach and clarity by ensuring that information security roles and responsibilities are defined and clearly articulated via policy documents, contracts and job descriptions and that understanding is reinforced through monitored training, documented procedures, probation and annual performance development reviews, such that all individuals understand their role and responsibility with respect to information security.

4.2.4 The University will ensure that information security knowledge is shared and appropriate information security controls applied in the most efficient, effective and economical manner by maintaining high level oversight via a co-ordinating body; by embedding information security considerations into service design, transition, and delivery; and by making the necessary tools and advice on information security available throughout the University, such that all individuals can access the relevant advice, policy, procedure, training or tools in a timely manner.

4.2.5 In order to reduce the number and severity of information security incidents, and to ensure that appropriate steps are taken with respect to reporting to relevant external authorities, information security incident recording, reporting and management system will be implemented and monitored, with outcomes informing future risk assessments.

4.2.6 A supportive culture for information security will be created within the University through clear management direction and demonstrated individual management commitment to the information security framework, including acknowledgement and explicit assignment of information security responsibilities, commitment to training uptake and reporting of security incidents.

4.2.7 The University will ensure that its information security framework is fit for purpose by utilising ISO/IEC 27001:2013 Information Security Management Systems Requirements, conducting regular audits and by a process of continual improvement, benchmarking itself with respect to information security against comparator institutions where possible.

5. GOVERNANCE AND RESPONSIBILITIES

5.1 Board of Governors

The Board has ultimate accountability for information security activities within the University. More specifically, it protects institutional reputation by being assured that clear regulations, policies and procedures that adhere to legislative and regulatory requirements are in place, ethical in nature, and followed. The Board needs to be assured that there are effective systems of control and risk management, and that governance structures and processes are fit for purpose by referencing them against recognised standards of good practice.

5.2 Vice Chancellor's Board

The University's Vice Chancellor's Board is responsible via the Vice-Chancellor to the Board of Governors for:

- leading and fostering a culture that values, protects and uses information for the success of the University and benefit of its members;
- defining the University's information security risk appetite in the context of the prevailing legal, political, socio-economic and technological environment and external standards;
- ensuring that a fit for purpose and adequately resourced information security framework is in place, including this policy as the top level reference document.

5.3 Senior Information Risk Owner

A Senior Information Risk Owner (SIRO) for the University's overall information security objectives shall be designated by the Vice-Chancellor, supported by a Deputy SIRO. The SIRO shall be a member of the University Executive Board. The key responsibilities of the SIRO shall be to:

- ensure that this policy and the information security objectives are compatible with the strategic direction of the University;
- ensure that data and information assets are identified; that the top level data and information governance roles are allocated and that the post-holders are appropriately briefed on their information security roles and carry out their functions with due diligence;
- own the risks associated with the information security objectives and ensure that control action owners are identified;

- ensure that exception procedures are in place to authorise at an appropriate level acceptance or mitigation of significant information security risks that deviate from agreed standards;
- determine when and by whom breaches of information security shall be reported to relevant external authorities;
- ensure there is clear direction and visible management support for security initiatives and promote continual improvement;
- ensure the Vice-Chancellor and Council are adequately briefed on risk management issues.

5.4 Information Governance Committee

The Information Governance Committee is responsible for providing strategic direction and focus to the activities of data and information management across the University. The scope includes information security and data quality.

The Information Governance Committee provides assurance to the University Vice Chancellor's Board via the Senior Information Risk Owner. The terms of Reference are set out in **(Appendix 2).**

5.5 Data & Information Governance Roles

Supporting Data & Information Governance roles shall be established by the Senior Information Risk Owner **(Appendix 3)**

5.6 Heads of Schools/Service Areas

Responsible for:

- ensuring that staff are aware of the need to adhere to this policy and associated information security policies;
- reporting non-compliance via the defined and approved channels.

5.7 All users

All individual users of University information systems and those handling or having access to University information outside of those systems shall be responsible for:

- complying with all relevant information security, policies, practices and procedures including any external accountability;
- ensuring that they request, where necessary, and receive adequate and relevant information security awareness training to enable them to undertake their roles; and
- reporting information security incidents via the defined and approved channels.

5.7 Information Asset Owners

Can be viewed on http://www.glyndwr.ac.uk/data-protection/IAOs

6. BREACHES OF POLICY

Breaches of the Information Security Policy may be treated as a disciplinary matter dealt with under the University's staff disciplinary policies or the Student Disciplinary Code as appropriate.

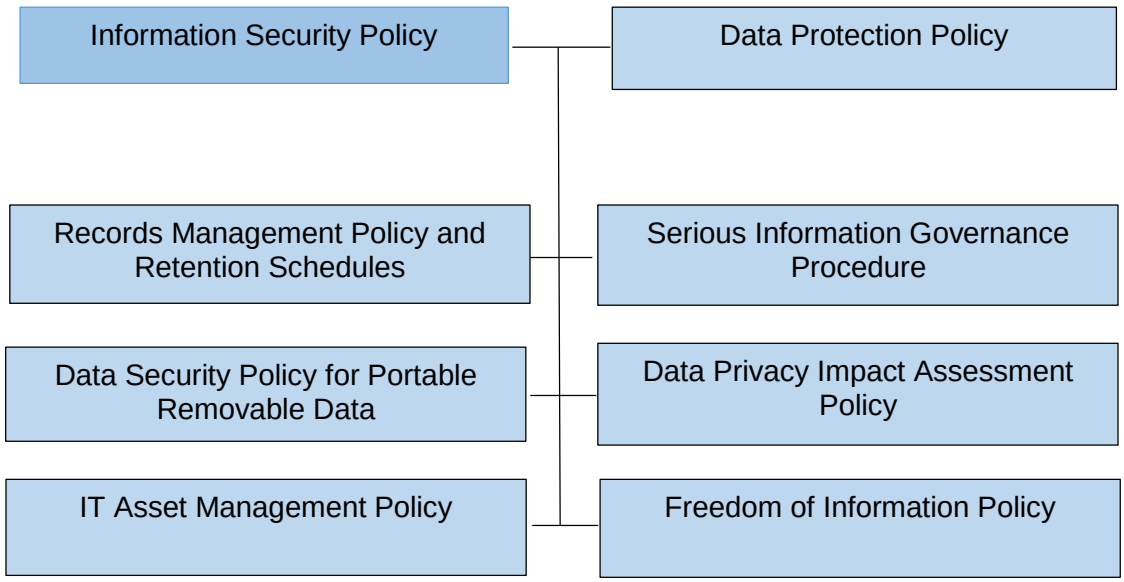
7. DEFINITIONS

Availability	Having appropriate access to Information Assets as and when required in the course of University business
Confidentiality	The restriction of information to those persons who are authorised to receive or access it
Information	Data that has a meaning or can be interpreted. It can be held as an electronic record or in a non-electronic format such as paper, microfiche, photograph
Information Asset	Information that has value to the University. Key Information Assets are the most important types of information required for achievement of the University's strategic aims
Integrity	The completeness and preservation of information in its original and intended form unless amended or deleted by authorised people or processes
Quality	The state of completeness, validity, consistency, timeliness and accuracy that makes data appropriate for both operational and strategic use.

APPENDIX 1

THE POLICY FRAMEWORK

The University's information security is managed through the below Policy Framework which comprises of This Policy and other relevant policies. This framework provides a flexible and effective platform upon which the University's information security objectives are met. The framework enables local autonomy in how the outcomes and objectives of this Policy are met, by allowing local procedural methods and/or controls to be implemented. At the same time, it allows those who require further advice from the Information Security Owner or the Data Protection Officer to meet this policy through methods detailed in the procedures. Regardless of this approach, all within scope of the Policy are required to meet this Policy and the other Policies outlined below using appropriate methods.



APPENDIX 2

INFORMATION GOVERNANCE COMMITTEE TERMS OF REFERENCE

The Information Governance Committee was established in April 2018 (the former information governance steering group is now dissolved). The Committee is chaired by the Senior Information Risk Officer (SIRO), designated by the Vice-Chancellor as the Director of Human Resources. The Committee consists of members at a senior management and appropriate level.

1. **Strategy –** To provide strategic direction for cultural change, conscious of the need for secure working practices, embracing a process of openness, learning and improvement in matters associated with Information Governance and ensuring adherence to good practice and the availability of high quality information at the point of service delivery
2. **Management of Risk -** Oversee the management of risks and implementation of strategies/policies associated with legislation and monitor compliance against such legislation and that it is embedded in the business planning, service management and risk management agendas
3. **Data Sharing -** Ensure that systems are in place to identify high-risk areas of information processing that require policy review, data sharing agreements and data privacy impact assessments.
4. **Data Quality -** Promote and engender a culture of data quality improvement and quality assurance that supports students and achieves a balance between secure working environment and efficiency and effectiveness within responsive timely and well supported service provision
5. **Data Breaches -** Receive reports, and make recommendations on actions, following any serious breaches of confidentiality and security (Data Protection Act) or any matter referred to the Information Commissioners Office and where appropriate undertake or recommend remedial action in accordance with the SIGI procedure
6. **Policies and Procedures -** Ensure that Data Protection, Freedom of Information and other information governance policies and procedures are established to comply with all relevant legislation and that all such policies and procedures are periodically assessed and audited.
7. **Safeguarding -** Ensure that the acquisition, deployment and operational use of manual and electronic systems of data and information management are underpinned by appropriate safeguards, with specific reference to the statutory environment
8. **Open and Transparent Processes -** Develop open and transparent processes governing the collection, handling and sharing of personal information
9. **Freedom of Information -** Receive and consider reports regarding all internal FOI reviews
10. **Information Security -** Ensure that the sharing of student/staff identifiable data is technically secure and underpinned by relevant guidance on consent and the circumstances where sharing is appropriate and lawful
11. **Administration Records -** Ensure that the University manages the safe retention, disposal, storage and retrieval of relevant records on time and at the right place, developing and promoting standards of good practice to improve information quality and records management
12. **Communications -** Develop and implement a communications programme to raise awareness within the University, and with others as appropriate, about all aspects of Information Governance, providing appropriate advice in response to events and incidents and follow necessary reporting, policies and procedures (SIGI Procedure)
13. **Training-** Ensure that training and awareness programmes are in place to equip staff with the skills and behaviours necessary to ensure compliance with good practice

Modus Operandi

- The IGC shall report to the VCET matters that are appropriate within its jurisdiction.
- The IGC shall produce an annual information governance improvement plan and monitor its implementation
- The ICG shall refer to the VCB, as appropriate, matters which require further debate and consideration.
- The ICG shall refer to Academic Board matters that are appropriate, within its jurisdiction.
- The ICG shall, at all times, work within the policies and procedures of the University.
- The ICG shall meet 4 times a year.

Membership

SIRO (Chair)	1
Deputy SIRO ,	1
Deputy Vice-Chancellor	1
Pro Vice-Chancellor	1
Director of Operations	1
Director of Finance	1
Legal Advisor	1
Total	**7**

Clerk

Data Protection Officer	**1**

Quorum: 5 (normally to include Chair or Vice Chair)

APPENDIX 3

INFORMATION GOVERNANCE ROLES