| | |
|---|---|
| **Teitl:**<br>**Title:** | **Polisi Diogelwch Gwybodaeth**<br>**Information Security Policy** |
| **Who does this Policy Relate to?**<br>**Who does this Policy Relate to?** | Myfyrwyr a staff<br><br>Students and staff |

Cydraddoldeb ac Amrywiaeth / Equality & Diversity

| | |
|---|---|
| Dolen at Gam 1 Asesu'r Effaith ar Gydraddoldeb: / Equality Impact Assessment Stage 1 Link: | |
| Dolen at Gam 2 Asesu'r Effaith ar Gydraddoldeb: / Equality Impact Assessment Stage 2 Link: | |
| Cynllun Gwella Asesu'r Effaith ar Gydraddoldeb / Equality Impact Assessment Improvement Plan | |
| *Effaith ar yr Iaith Gymraeg*<br><br>*Mae asesiad effaith wedi'i gynnal ar y polisi hwn i ystyried ei effaith ar yr Iaith Gymraeg yn unol â Safonau'r Gymraeg (94-104) a Mesur yr Iaith Gymraeg (Cymru) 2011.* | *Welsh Language Impact*<br><br>An impact assessment has been carried out on this policy to consider its effect on the Welsh Language in accordance with the Welsh Language Standards (94-104) and the Welsh Language (Wales) Measure 2011. |

Adolygu a Chymeradwyo / Review and Approval

| | |
|---|---|
| **Perchennog y Ddogfen:**<br>**Document Owner:** | *Chief Operating Officer/Deputy Chief Executive* |
| **Ymgynghoriad:**<br>**Consultation:** | *ISPG* |
| **Corff Cymeradwyo:**<br>**Approval Body:** | *ISPG* |
| **Dyddiad Cymeradwyo:**<br>**Approval Date:** | 27/06/2020 |
| **Dyddiad Adolygu:**<br>**Review Date:** | *27/06/2023* |
| **Fersiwn:**<br>**Version** | *1.2* |

## Table of contents

# 1. Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the on-going functioning of Coleg Cambria. Failure to adequately secure information increases the risk of financial and reputational losses.

This overarching policy provides an overview of information security and lists a set of policy documents (sub-policies) which - taken together - constitute the Information Security Policy of the College.

# 2. Purpose

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which would otherwise occur.

# 3. Scope

The documents in the Information Security Policy set apply to all information assets which are owned by the College, used by the College for business purposes or which are connected to any networks managed by the College. The documents in the Information Security Policy set apply to all information which the College processes, irrespective of ownership or form. The documents in the Information Security Policy set apply to all members of the College and any others who may process information on behalf of the College.

# 4. Structure

The Information Security Policy document set is structured in accordance with the recommendations set out in the “UCISA Information Security Toolkit” which in turn, is based on the control guidelines set out in the industry standard ISO 27001. This top level document lists a set of other sub-policy documents which together constitute the Information Security Policy of the College.

Each of the sub-policy documents contains high-level requirements and principles. They do not, and are not intended to include detailed descriptions of policy implementation. Such details will, where necessary, be supplied in the form of separate procedural documents which will be referenced from the relevant, individual sub-policy documents.

## 5. Information Security Principles

The College has adopted the following principles, which underpin this policy:

1. Information will be protected in line with all relevant College policies and legislation, notably those relating to data protection, human rights and freedom of information.

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 and mitigate any associated information risks.

3. Information will be made available solely to those who have a legitimate need for access.

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.

## 6. Monitoring and Review

- Responsibility for the production, maintenance and communication of this top level policy document lies with the College's Chief Operating Officer/Deputy Chief Executive, as the organisation's Senior Information Risk Owner (SIRO).

- This top-level policy document has been approved by the College's Governing Body. Substantive changes to this policy may only be made with the further approval of the Governing Body.

- Responsibility for the production, maintenance and communication of all sub-policy documents lies with the College's Director of Technology.

- Responsibilities for the approval of all sub-policy documents are delegated to the College's Risk Management Group. Any significant changes will be reviewed by the

College's Information Security and Privacy Group (ISPG) prior to approval. ISPG comprises representatives from all relevant parts of the organisation.

- Each of the documents constituting the Information Security Policy will be reviewed every 3 years or more frequently as required.
- Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.

## 7. Policy Documents

| Name | ID |
|---|---|
| **Information Security Policy (This Document)** | ISP001 |
| Legal, Regulatory & Contractual Frameworks Policy | ISP002 |
| Acceptable Use Policy | ISP003 |
| Mobile & Remote Working Policy | ISP004 |
| Information Handling Policy | ISP005 |
| Encryption Policy | ISP006 |
| Network Management Policy | ISP007 |
| User Management Policy | ISP008 |
| Antivirus & Malware Policy | ISP009 |
| Patch Management Policy | ISP010 |
| Outsourcing and Third Party Compliance | ISP011 |
| System Management Policy | ISP012 |
| Investigation of Computer Use Policy | ISP013 |
| Software Management Policy | ISP014 |
| Data Protection Policy | ISP015 |

## 8. Change History

| Version no. | Effective Date | Significant Changes |
|---|---|---|
| **1** | **28/06/2017** | **New Policy** |
| **1.1** | **19/04/2018** | **Added Data Protection Policy as sub-policy** |
| **1.2** | **27/06/2020** | **Reviewed by ISPG - No significant changes** |
| | | |