Teitl: **Title:**	**Polisi Diogelu Data** **Data Protection Policy**
Who does this Policy Relate to? **Who does this Policy Relate to?**	Myfyrwyr a staff 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 *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* 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: **Document Owner:**	*Chief Operating Officer/Deputy Chief Executive*
Ymgynghoriad: **Consultation:**	*Information Security and Privacy Group (ISPG)*
Corff Cymeradwyo: **Approval Body:**	*Governing Body*
Dyddiad Cymeradwyo: **Approval Date:**	27/06/2020
Dyddiad Adolygu: **Review Date:**	27/06/2023
Fersiwn: **Version**	*1.5*

Table of contents

1. Introduction

Coleg Cambria holds and processes information about employees, students, and other data subjects for academic, administrative and commercial purposes. In achieving this mission and as part of its daily operations, the College takes the protection of the personal data it processes extremely seriously.

The College will take reasonable and proportionate measures to ensure that it protects personal data against accidental or deliberate misuse, damage or destruction. It is also committed to a policy of protecting the rights and freedoms of all individuals, in relation to the processing of their personal data, in compliance with UK Data Protection legislation.

2. Purpose

The purpose of this policy is to ensure that all members of the College comply with the provisions of UK Data Protection legislation (i.e. Data Protection Act 2018 and the General Data Protection Regulation (enforced May 2018) when processing personal data. Any serious infringement of the Act/Regulation will be treated seriously by the College and may be considered under disciplinary procedures. A serious breach of the Data Protection Act or GDPR may also result in the College and/or the individual being held liable in law.

3. Scope

The College processes personal information to enable us to provide education and support services to our students; process employment details of staff; manage our accounts and records; provide commercial activities to our clients; advertise and promote the college and the services we offer. We also process personal information through CCTV systems that monitor and collect visual images for the purposes of safeguarding, security and the prevention and detection of crime. This policy applies regardless of where the personal data is held or whether it is held physically or electronically.

This Policy applies to all members of the College and any others who may process personal data on behalf of the College.

4. Principles

The College adheres to the principles of the European General Data Protection Regulation and the UK Data Protection Act 2018. In accordance with these principles, personal data shall be:

General Data Protection Regulations Principles	
Lawfulness, fairness and transparency	Processed lawfully, fairly and in a transparent manner in relation to individuals.
Purpose limitation	Data collected for specified, explicit and legitimate purposes and not further processed in a manner that is 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.
Data minimisation	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Accuracy	Accurate and where necessary, kept up to date; whilst having regard to the purposes for which data is processed, every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
Storage limitation	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.
Integrity and confidentiality	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 GDPR introduces an ‘accountability’ principle, this ensures that the Data Controller (the College) is responsible for, and can demonstrate and verify their compliance with data protection legislation.

5. Responsibilities

All

The College expects all its members to comply fully with its Data Protection Policy and the law. Further details of responsibilities can be found in the Coleg Cambria Data Protection RACI Matrix.

Managers

The Senior Management Team (SMT) and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice and promoting the privacy rights of data subjects within the College. Certain managers will have additional responsibilities for data protection, based on their role within the organisation. These are defined in the College's Data Protection RACI Matrix.

Data Protection Officer

Data Protection Officer is responsible for day-to-day data protection matters and will perform the following tasks:

- inform and advise the College and its employees about their obligations to comply with the GDPR and other data protection laws.
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, students, etc.).

Staff

Staff are responsible for:

- ensuring that all the personal data the College holds about them in connection with their employment is accurate and up-to-date;
- informing the College of any changes or errors to information which they have provided immediately, e.g. change of address either via CIPHR or other appropriate channels, dependent on the circumstances;
- ensuring, where they process personal data in connection with their employment and are permitted to do so under the College's notification to the ICO, that any personal data processed is kept securely and is not disclosed either orally or in writing to any unauthorised third party;
- informing the Data Protection Officer (dpo@cambria.ac.uk) if they intend to process personal data for a new purpose, transfer personal data to a new data processor or undertake any significant changes to the management or handling of personal data. Where any of these activities are to be undertaken a Privacy Impact Assessment (PIA) of this new or additional processing, must be completed to ensure compliance with data legislation prior to the processing of personal data. As part of the PIA staff need to provide full details of the type of personal data to be processed (e.g. financial details, contact details, etc.), who the subject of the data is (students, staff, the public, etc.), why the data is being processed (marketing, staff administration, etc.)

and whether the intention is at any time to transfer the data to a third party who is not the subject of the data, including whether this is an international partner.

Anyone responsible for creating or maintaining web pages should note that College Policy and the provisions of data protection legislation will relate to any personal data about individuals that may be held on web pages or accessed via them.

Students

Students must ensure that any information they provide to the College is accurate and is kept up-to-date. If they find themselves in a position where they are processing personal data about staff or other students, then they must comply with College Policy and the law.

Any students at Coleg Cambria who handle or process personal data about individuals (names, contact details, financial details, course details, personal circumstances, beliefs etc.) in the course of their studies must be aware of the processing principles and how to apply them.

Further clarification can be sought from the DPO at dpo@cambria.ac.uk.

Others

Other stakeholders, contractors, visitors, or others who provide personal data to the College or process personal data on behalf of the College must also comply with College Policy and the law.

6. Data Subject Rights

Under the Data Protection Act 2018 individuals have a right to inspect or request all personal information held about them. This can include, for example, the contents of student files, staff files, enrolment forms, HR records. Data subjects might include staff, students, alumni, job applicants, former employees, members of the College Board of Governors and members of the public.

Under the General Data Protection Legislation (GDPR), data subjects rights have been expanded. They are as follows;

- The Right to be Informed - subjects should understand the data they are submitting and how it will be processed.
- The Right of Access - subjects should have access to their data that is held by the Data Controller, if they request it.
- The Right to Rectification - subjects can request that incorrect personal data be rectified.
- The Right to Erasure (a.k.a. The “Right to be Forgotten”) - subjects can request the erasure of their personal data if there are no legitimate grounds for the Controller to

retain it.

- The Right to Portability - the Data Controller should move the subject's data to another controller for further use.
- The Right to Object - subjects can object to the processing of their data if they suspect the grounds for doing so are not legitimate.

The College is committed to the management of such requests and any individual wishing to obtain personal information about themselves or exercise their rights under GDPR should contact the Data Protection Officer at dpo@cambria.ac.uk.

7. Privacy Notices

Where the College obtains data directly from a data subject the College must provide information about the processing of personal data that is:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The GDPR sets out the information that the College should supply to individuals:

- Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer.
- Purpose of the processing and the lawful basis for the processing.
- The legitimate interests of the controller or third party, where applicable.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and safeguards.
- Retention period or criteria used to determine the retention period.
- The existence of each of the data subject's rights.
- The right to withdraw consent at any time, where relevant.
- The right to lodge a complaint with the supervisory authority.
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.
- The existence of automated decision-making (including profiling) and information about how decisions are made, their significance and their consequences.

8. Obtaining Consent

Personal data or sensitive data should not be obtained, held, used or disclosed unless the College has a legal basis for doing so and this may require consent from the individual.

The College will also process specified classes of personal data to fulfil contractual requirements. This is a condition for acceptance of a student on to any course, and as a condition of employment for staff.

If personal data is to be used for direct marketing purposes then the data subject must be informed of this at the time of collection and must positively opt-in to the correspondence.

9. Definitions

“Personal Data” Any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

“Sensitive / Special Category Data” Any information that relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, or criminal convictions. Sensitive data are subject to much stricter conditions of processing.

“Data Controller” Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

“Data Subject” Any living individual who is the subject of personal data held by an organisation.

“GDPR” The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

“Processing” Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data, accessing, altering, adding to, merging, deleting, data retrieval, consultation or use of data disclosure or otherwise making data available.

“Third Party” Any individual/organisation other than the data subject, the data controller or its agents.

“Staff” Any person employed by the College including past, present and prospective employees.

“Students” Any person attending a course at the College including past, present and prospective students.

10. Related Documents

This Policy should be read in conjunction with other College Policies and procedures. The following documents are relevant to this Policy:

- ISP001 Information Security Policy
- ISP005 Information Handling Policy

- ICTSOP-024 Information Security Incident Management Procedure
- ICTSOP-033 Procedure for Responding to a Data Breach
- Privacy Impact Assessment Template
- Outsourcing and Third Party Compliance
- Data Protection RACI Matrix

11. Monitoring and Review

- Responsibility for the production, maintenance and communication of this 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 Data Protection Officer.
- Responsibility for the approval of all sub-policy documents is 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.
- The Data Protection 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.

12. Change History

Version no.	Effective Date	Significant Changes
1	**04/05/2016**	**New Policy**
1.1	**12/03/2018**	**Updated to include requirements of the GDPR**
1.3	**19/04/2018**	**Updated approval by Governing Body**
1.4	**30/10/2019**	**Updated responsibilities, added RACI Matrix & removed reference to Data Protection Act 1998**
1.5	**27/06/2020**	**Reviewed with no changes**