Teitl: Polisi Diogelu Data
Title: Data Protection Policy

Dyddiad Cyhoeddi:
Issue Date: 19/04/2018

Adolygu a Chymeradwyo / Review and Approval

Cyfrifoldeb: **Responsibility:**	*Chief Operating Officer/Deputy Chief Executive*
Corff Cymeradwyo: **Approval body:**	*Governing Body*
Dyddiad Cymeradwyo: **Approval date:**	*10/10/2018*
Amlder Adolygu: **Review Frequency:**	*3 Years*
Dyddiad Asesu'r Effaith ar Gydraddoldeb: **Equality Impact Assessment Date:**	*09/04/2018*
Dyddiad y Daw i Ben: **Expiry Date:**	*18/04/2021*

Cwmpas / Scope

Sicrhewch fod y polisi/strategaeth yn cynnwys datganiad cwmpas sydd yn nodi at bwy neu beth mae'r polisi yn berthnasol iddynt. Er enghraifft: pob gweithiwr, myfyriwr, system gyfrifiadurol, taliad cerdyn credyd.
Please ensure that the policy/strategy includes a scope statement that specifies to who or what the policy applies. For example: all employees, all learners, all computer systems, all credit card payments.

I'w bennu gan y Rheolwr Gweinyddol a Gwasanaethau Cwsmeriaid /
/ To be assigned by the Admin & Customer Service Manager

Cyfeirnod: **Reference:**	*Ceir ei bennu wedi cymeradwyo'r ddogfen* *This will be assigned to the document on approval*
Fersiwn: **Version:**	*1.4*
Dosbarthiad: **Classification:**	*Dogfen Arferol* *Normal*

Coleg Cambria

Data Protection Policy

Title:	**Data Protection Policy**
Reference:	**ISP015**
Version:	**1.4**
Approval Date:	**10/10/2018**
Issue Date:	**19/04/2018**
Classification:	**Normal**

Introduction

Coleg Cambria holds and processes personal data 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.

Purpose

The purpose of this policy is to ensure that when processing personal data all members of the College comply with the provisions of Data Protection Legislation (i.e. Data Protection Act 2018 and the General Data Protection Regulation (the Regulation) (enforced May 2018 replacing the Data Protection Act 1998) and all and any other laws which protect and govern the processing of personal data). Any serious infringement of any Data Protection Legislation will be treated seriously by the College and may be considered under disciplinary procedures. A breach of the Data Protection Legislation may also result in the College and/or the individual being held liable in law.

Scope

The College processes personal data 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 data 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 manually or electronically.

This Policy applies to all members of the College and any others who may process personal data on behalf of the College, who must comply with College Policy, the law and the terms of contracts and agreements which are in place for the provision or processing of the data.

Principles

The College adheres to the principles of the current Data Protection Legislation. In accordance with these principles personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.

- 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.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- 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.

- 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 GDPR in order to safeguard the rights and freedoms of individuals.

- GDPR does not contain a specific principle relating to individuals' rights - these are specifically addressed in separate articles (if you would like more information, please see GDPR Chapter III - https://gdpr-info.eu/chapter-3/).

- 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.

- GDPR does not contain a specific principle relating to overseas transfers of personal data - these are specifically addressed in separate articles (if you would like more information, please see GDPR Chapter V - https://gdpr-info.eu/chapter-5/).

In addition the GDPR introduces an ‘accountability’ principle, this ensures that Data Controllers (e.g. Coleg Cambria) are responsible for, and can demonstrate and verify their compliance with personal data legislation.

Responsibilities

All

The College expects all its members to comply fully with its Data Protection Policy and all relevant Data Protection Legislation.

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.

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 Data Protection Legislation.
- monitor compliance with Data Protection Legislation, 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, customers 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 Carval or other appropriate channels, dependent on the circumstances;

- Ensuring that where they process personal data as part of their job - 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;

- ensuring that they complete mandatory training for information security and data protection;

- consult with the Data Protection Officer (dpo@cambria.ac.uk) if they plan 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 Data Protection Impact Assessment (DPIA) of this new, or additional processing, must be completed to ensure compliance with data legislation prior to the processing of the personal data. As part of the DPIA staff need to provide full details of the type of personal data to be processed (i.e. 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 external to the College 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 the College's information security and data protection policies 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 the College's information security and data protection policies 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, the law and the terms of contracts and agreements which are in place for the provision or processing of the data.

Data subjects rights

Under the Data Protection Legislation individuals have a right to inspect or request all personal data 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 College Board of Governors and members of the public.

Under the Data Protection Legislation , 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 ground for doing so are not legitimate

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

The College does not perform any automated decision-making or profiling in its operations.

The use of cloud service provision, such as the Coleg Cambria Google platform, may result in transfers of personal data to third countries and is subject to contracts and appropriate safeguards to ensure data protection.

The College may also transfer personal data to third countries to fulfil its international activities, such as arranging placements for students abroad or providing training or placements for overseas students. This will only take place where prior consent has been obtained, or where it forms part of a contract with the data subject.

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 country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a 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, the significance and the consequences

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. Where consent must be sought for processing personal data, the College will obtain it from the individual at the time of data capture.

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.

Definitions

"Personal Data" Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. includes name, address, telephone number, id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

"Sensitive Data" Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing. GDPR defines *Sensitive Data* as *Special Category Data*.

“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 available of data.

“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 potential employees.

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

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
- Completing a Data Protection Impact Assessment (DPIA)
- Outsourcing and Third Party Compliance
- Data Protection RACI Matrix
- Information Retention Schedule

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 Governing Body.
- Responsibilities 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.

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	**28/09/2018**	**Removed references to Data Protection Act 1998 (superseded by GDPR and DPA 2018)**