

Data Protection Policy

Mae'r ddogfen hon ar gael yn y Gymraeg / This document is available in Welsh

Prepared by:	Vice Principal / Data Protection Officer	
Policy Approved by:	Senior Leadership Team	24/10/18
		21/10/18
		18/10/22
	Data Protection group	08/11/18
		08/11/18
	Compliance group	21/10/21
		21/10/22
	Audit committee	22/02/16
		26/11/18
		28/11/22
Impact Assessed	October 2018, October 2022	
Reviewed:	November 2015, September 2018, October 2021, October 2022	
Review Date:	September 2022, September 2024	

Contents

Page 3	1. Introduction
Page 6	2. Status of the Policy
Page 6	3. Notification of Data Held and Processed
Page 6	4. Responsibilities of Staff
Page 7	5. Data Security
Page 7	6. Learner Obligations
Page 8	7. The Rights of Access
Page 9	8. Subject Consent
Page 9	9. Processing Sensitive Information
Page 10	10. The Data Controller and the Data Protection Officer and Data Controller
Page 10	11. Retention and Deletion of Data
Page 11	12. Information Sharing Protocols
Page 11	13. Conclusion
Page 12	Appendix 1 – Role of Data Controllers

1. Introduction

1.1 The College needs to collect and keep certain data about its employees, learners and other users to allow it to exercise its function effectively. This includes monitoring its performance, organise learning provision, record learners' achievements, and maintain financial, health and safety and employment records.

1.2 The College collects data to meet its obligations to funding bodies and ensure government (and for example European) rules are complied with in respect of funding, e.g. to support financial audit requirements (see 1.2 above). Data collected also supports the process of staff recruitment and to facilitate payment of salaries and in some instances the payment of learner grants.

1.3 Under certain conditions of some financial grants, the College needs to share data with other public sector organisations. Staff and learners will be informed of when this could happen, and the steps taken to ensure that no personal data that could identify the individual is transferred and when personal data is required specific consent is received.

1.4 This policy aims to mitigate the risk to the security of data. Data is mainly obtained and processed from individuals and organisations mainly in College Functional or Business Support Departments that include Learner & Campus Services, People & Culture, Exams and Management Information Systems, and Finance.

1.5 The College also collects data via its CCTV system to enable it to perform its functions in respect to both health and safety responsibilities and the prevention of crime.

1.6 The College will do its utmost to ensure that the data collected is used fairly, stored safely and not disclosed to any other person unlawfully. Data will be deleted safely when the duration that the data is held for it to comply with the law expires.

1.7 The College must comply with the Data Protection Principles that underpin Data Protection Act 2018 (the 2013 Act) and the General Data Protection Regulation. In summary these state that personal data shall:

- a) Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- b) Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- c) Be adequate, relevant and not excessive for those purposes.
- d) Be accurate and kept up to date.
- e) Not be kept for longer than is necessary for that purpose.
- f) Be processed in accordance with the data subject's rights.
- g) Be kept safe from unauthorised access, accidental loss or destruction.

h) Not be transferred to a country outside the EU, unless that country has equivalent levels of protection for personal data.

1.8 Individuals have the following rights in relation to the 2018 Act:

- i. The right to be informed
- ii. The right of access
- iii. The right to rectification
- iv. The right to erasure
- v. The right to restrict processing
- vi. The right to data portability
- vii. The right to object
- viii. Rights in relation to automated decision making and profiling

The Right To Be Informed

Individuals have the right to be informed about the collection and use of their personal data. The College will provide individuals with information including the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. This is called 'privacy information'.

The Right Of Access

Individuals have the right to access their personal data and the right of access allows individuals to be aware of and verify the lawfulness of the processing of their data. Requests for such information will be known as Subject Access Requests.

The Right To Rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. The College will respond to such requests within one calendar month.

The Right To Erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. The right is not absolute and only applies in certain circumstances. The College will respond to such a request within one month.

The Right To Restrict Processing

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, the College is permitted to store the personal data, but not use it.

The Right To Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The Right To Object

The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing.

Rights in relation to automated decision making and profiling.

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Automated individual decision-making is making a decision solely by automated means without any human involvement.

Profiling is defined as:

“Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

1.9 The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. To ensure that this happens, the College has developed this Data Protection Policy.

1.10 The Freedom of Information Act 2000 gives a general right of access to all recorded information held by public authorities. However, this Act also sets out exemptions to that right and such exemptions include individual information on staff and learners by virtue of being personal information.

2. Status of the Policy

2.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

2.2 Any member of staff, who considers that the policy has not been followed in respect of personal data about THEM, should raise the matter with the designated data controller initially. If the matter is not resolved, it should be raised as a formal grievance.

3. Notification of Data Held and Processed

3.1 All staff, learners and other users are entitled to know

- what information the College holds and processes about them and why
- how to gain access to it,
- how to keep it up to date and
- what the College is doing to comply with its obligations under the 2018 Act and the GDPR.

3.2 The College will therefore provide all staff and learners and other relevant users with a privacy notice. This will state the types of data the College holds and processes about them, and the reasons for which it is processed. The College will, as part of the Employment Contract Process, seek specific consent from employees to process data relating to them.

4. Responsibilities of Staff

4.1 All staff are responsible for:

4.1.1 Checking that any information that they provide to the College in connection with their employment is accurate and up to date and informing the College of any changes to information, which they have provided e.g., changes of address.

4.1.2 Checking the accuracy of the information the College sends out from time to time, giving details of information kept and processed about staff.

4.1.3 Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

4.1.4 If, and when, as part of their responsibilities, staff collect information about other people. (e.g., learners' personal details, data relating to learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are at appendix 1.

4.1.5 Notifying their line manager (who subsequently should inform the Data Protection Officer of any suspected or actual breaches in data security that may lead to data loss relating to staff, learners or organisations.

5. Data Security

5.1 All staff are responsible for ensuring that any personal data they hold (for example of learners, staff or other organisations) is kept securely and that personal information is not disclosed either orally or in writing, electronically, or accidentally or otherwise to any unauthorised third party.

5.2 Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct.

5.3 Personal information should be kept in a locked filing cabinet, or in a locked drawer, or if it is computerised, be password protected. To reduce risk to data users should store computerised data within the provided resources such as Office 365 or mapped network drives.

Portable hard-drives or pen-drives should be used as last resort. If used, these portable devices should be encrypted. Staff should seek technical advice from IT Dept. if they are unfamiliar with such processes.

5.4 Staff should NOT remove personal data relating to other staff, organisations or learners from college premises. This includes data kept on disk drives, electronic transmission to their home or other venues even if the data is to be used for work purposes.

5.5 The College will do its utmost to protect personal data held electronically-digitally on its computers and servers, this includes ensuring that all security software and other technical protection is enacted to diminish the risk of access to data, including remotely (e.g., via the internet).

5.6 The College will notify the ICO of any breach of security and management of held data. In the event that a breach has occurred the College shall implement its Breach Management Plan.

6. Learner Obligations

6.1 Learners must ensure that all personal data provided to the College is accurate and up to date. If learners need to change any personal data, they have to complete a 'Change of Details' form and submit this to the Campus Office.

7. The Rights of Access

Individuals have the right to access their personal data and the right of access allows individuals to be aware of and verify the lawfulness of the processing of their data. Requests for such information will be known as Subject Access Requests.

All Subject Access Requests must be submitted to:

Data Protection Officer

Coleg y Cymoedd Twyn Rd, Ystrad Mynach, HENGOED CF82 7XR

T: 01443 810053

E: Data-protection@cymoedd.ac.uk

The College will provide a copy of the information free of charge. Information will be provided within one month of receipt of the request. The College will ensure that the identity of the person making the request is verified, using reasonable means.

The College will charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that the College will charge for all subsequent access requests.

The fee will be based on the administrative cost of providing the information. Individuals will be given an indicative cost at the time they make their application.

The College reserves the right to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case the College will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

If requests are manifestly unfounded or excessive, in particular because they are repetitive, the College will:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where the College refuses to respond to a request it will explain why to the individual, informing them of their right to complain to the ICO within one month.

If the request is made electronically the College will provide the information in a commonly used electronic format.

8. Subject Consent

8.1 In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

8.2 Some jobs or courses will bring the applicants into contact with children. The College has a duty under the Children's Act and other enactments to ensure that staff are suitable for the job, and learners for the courses offered. The College also has a duty of care to all staff and learners and must therefore make sure that employees and those who use the College's facilities do not pose a threat or danger to other users.

8.3 The College will also ask for information about particular health needs, such as allergies to certain forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual but will need consent to process in the event of a medical emergency, for example.

9. Processing Sensitive Information

9.1 Sometimes it is necessary to process sensitive information, which may include information about a person's health, ethnic background, political opinions, religious beliefs, sexual health and criminal convictions. This may be to ensure the College is a safe place for everyone, or to operate other College policies such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and learners will be asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to give consent to this without good reason. More information about this is available from the Acting Director of People & Culture for staff and Director of MIS or Line Managers for learners.

10. The Data Controller and the Data Protection Officer and Data Controllers

10.1 The College as a body corporate is the Data Controller under the Act, and the Corporation Board is therefore ultimately responsible for implementation.

10.2 The Data Protection Officer has the following responsibilities:

- Provide continued guidance, support and leadership on current and impending data protection legislation and regulation across the College
- Identify and implement the work required to bring the College up to standards required by the GDPR and put in place processes to ensure continued compliance
- Carry out regular risk assessments of the handling of data and maintain and update the risk register
- Create and maintain data protection policies and procedures
- Maintain evidential records of compliance with current legislation
- Support a programme of staff awareness training, to deliver compliance and foster a culture of data privacy within the organisation
- Review commercial agreements and contracts including data processing agreements with existing and future data processors
- Revise and lead data breach response and notification procedures
- Be the point of contact and co-operate with the ICO
- Act as the focal point for the organisation when data subjects are exercising their rights; supervise and advise on the response to such requests

10.3 The College has several designated data controllers. They include the Acting Director of People & Culture, the Director of Exams & Management Information Services, Estates Manager, Campus Service Managers and Heads of Schools (see appendix 1)

10.4 The College also has several authorised staff in academic areas to manage and deal with sensitive data relating to learners.

11. Retention and Deletion of Data

11.1 The College will keep some forms of data for longer than others. Because of storage problems, information about learners cannot be kept indefinitely, unless there are specific requests to do so. In general, information about learners will be kept for a maximum of 7 years after they leave the College. However, it may be case that some data will have to be retained for a longer period to meet data retention requirements of such funding bodies as the EU. This will include name and address, academic achievements, including marks for coursework and copies of any reference written and name of employer.

11.2 All other information, including any sensitive information about health, ethnic background, political opinions, religious beliefs, sexual health, criminal records or disciplinary matters will be destroyed within a shorter period of the course ending and the learner leaving the College depending on circumstances.

11.3 In general all information will be kept for 4 years after a member of staff leaves the College. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding employment and information required for job references. A full list of information with retention times is available from the Director of People & Culture.

11.4 The College will safely destroy data, (e.g., using shredders on college premises) when it is no longer required and in line with the periods indicated above (see 13.1). For large quantities of documents containing personal and other data, the College shall only use recognised companies for this purpose. The College will employ similar approaches to the destruction of electronic data. When this is held on computer drives the College shall employ registered companies for this purpose specifically in relation to drives in PCs.

11.5 Data captured digitally via CCTV will normally be kept for 31 days and destroyed thereafter. The exception to this is when this data is required to support crime detection and subsequent legal proceedings

12. Information Sharing Protocols

The College may enter into data sharing arrangements with partner organisations from time to time. Where these occur, they will be arranged in line with the Wales Accord on the Sharing of Personal Information (WASPI). Copies of each information sharing protocol (ISP) can be obtained for the College's data controller on request.

13. Conclusion

13.1 Compliance with the 2018 Act is the responsibility of the College. Any deliberate breach of this Data Protection Policy may lead to disciplinary action being taken, or access to college facilities being withdrawn, or even criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should take it up with a designated data controller.

13.2 This policy will be reviewed every 2 years unless further legislation necessitates an earlier review date.

Appendix 1**Data Controllers**

The College has several designated data controllers. These are:

Area	Staff Name
Acting Director of People & Culture	Hannah Hallett
Estates Manager	Martin Donovan
Learner and Campus Office Managers	Lisa Condrón – Nantgarw Tim Leeke – Ystrad Mynach Becky Roberts – Aberdare Alexandra O'Brian – Rhondda
Director of EMIS	Russell Tuck
Director of Finance	David Francis
Heads of School	Simon Jenkins Dean Howells Julie Richards Jaye Lawrence Lee Davies Lauren Alexander Martin Watkins David Howells Hayley Hunt Kathryn E Bishop
ESF Team	Amanda Pearce