Policy	Data Protection (GDPR) Policy – ORG34
Document owner	Director of People & Resources
Date first implemented	February 2015
Date last reviewed	February 2024
Date of next review	February 2027
Date governor-approved	May 2018
Associated documents	Retention Policy & Schedule CCTV Policy Sharing Information Policy CLB (Acoustic Monitoring) Policy
Reference documents	Data Protection Breach Log
Initial reviewing body	Human Resources
Final approval body	Senior Leadership Team
Published on website	Yes

Purpose	This policy sets out the College's commitment to comply with the General Data Protection Regulations (GDPR).
Scope	Derwen College is required to process relevant personal data regarding members of colleagues, governors, volunteers, applicants, students/clients and their families, alumni, and customers as part of its normal operation and we shall take all reasonable steps to do so in accordance with this policy, the Data Protection Regulations and GDPR.
Equality, Diversity & Inclusivity	*"[Derwen] College is committed to promoting equality, good relations and to challenging discrimination. This is reflected in all College policies, procedures, processes, and practices." Derwen College Equal Opportunities Policy* Derwen College's ethos is to embrace diversity, to offer equality of opportunity, and to treat every individual fairly and with respect. Equality, diversity, and inclusivity are embedded throughout the organisation. This policy should be applied in accordance with this ethos. If you would like a copy of this document in a different format, such as large print, please contact the Human Resources Department who will provide help with alternative formats.

Data Protection Principles

The following principles of data protection will be applied at all data that is processed:

1. Personal data must be processed lawfully, fairly and in a transparent manner.
2. Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
4. Personal data must be accurate and, where necessary, kept up to date.
5. Personal data must not be kept for longer than is necessary.
6. Personal data must be processed in accordance with the data subjects' rights.
7. Personal data must be secure.
8. Personal data must not be transferred to another country (outside the EEA) without adequate protection.

Data Protection Control

The College has appointed the Director of People & Resources as the Data Protection Officer (DPO) who will endeavour to ensure that all data is processed in accordance with this policy and GDPR.

Our data processing activities are registered with the Information Commissioner's Office (ICO).

Personal and Sensitive Data

All data within the College shall be identified as personal, sensitive or both. This will ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of individuals to whom it relates.

Personal data covers both facts and opinions about an individual where that data identifies an individual. It includes information necessary for employment such as names, addresses, salary details or student attendance record or exam results. Personal data may also include sensitive personal data.

Sensitive personal data includes data relating to medical information, gender, religion, race, sexual orientation, trade union membership and criminal records.

Processing of Personal Data

The College will be transparent about the intended processing of data and communicate these intentions to all colleagues, students/clients, contractors, and

customers.

Consent may be required for the processing of personal data unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with consent.

Exemptions

Certain data is exempted from the provision of the Data Protection Act, data will be exempt for the following reasons:

- National security and the prevention or detection of crime
- The assessment of tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the College

Data Storage and Security

Hard copy data, records and personal data are stored out of sight and in a locked and secure filing cabinet.

Sensitive personal data should not be removed from college; however, the College acknowledges that colleagues may need to transport data between college and their home to access it for work when working from home, during the evenings and at weekends. This may also apply in cases where colleagues attend offsite meetings.

The following guidelines are in place to reduce the risk of personal data being compromised:

- Paper copies of data should not be taken offsite. If there is no way to avoid taking a paper copy, the data should not be on view in public places or left unattended under any circumstances.
- Unwanted paper copies of personal or sensitive data should be kept in the confidential waste bins provided in each building, where arrangements can be made for the documents to be collected and securely shredded. This also refers to handwritten notes if the notes reference any staff member or student by name.
- Care must be taken to ensure that any printout of any personal or sensitive data is not left in printer trays or photocopiers.
- If data is being viewed on a PC, colleagues must ensure that the window and documents are properly shut down before leaving the computer unattended.
- Sensitive data should not be viewed on public computers.
- If it is necessary to transport data away from college and/or our Satellites, it should be downloaded onto a USB stick (or another suitable secure device).

The data should not be transferred from this stick onto any home or public computer.
- USB sticks (or other suitable devices) must be password protected.
- Confidential e-mails should be sent via Egress.

All colleagues are responsible for ensuring that:

- any personal data that they hold is kept securely.
- personal information is not disclosed either orally, in writing or via web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
- they undertake the mandatory GDPR training to ensure understanding the amended data principles.

Personal information should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Unauthorised disclosure of data will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Disaster Recovery

- The College backs up data every evening.
- Master copies of software are stored off site or in a heat-proof safe.
- Firewalls and virus checkers are kept up to date and running.
- Computers are protected from physical harm, theft, or damage, and from electrical surges using protective plugs.

Subject Consent

The GDPR sets a high standard for consent and requires a positive opt-in. Neither pre-ticked boxes nor any other method of default consent is allowed. As required by the GDPR, the College takes a "granular" approach i.e., it asks for separate consent for separate items and will not use vague or blanket requests for consent. As well as keeping evidence of any consent, it can easily be withdrawn.

It should be noted, however, that consent is only one of the lawful bases on which data processing depends. The others include the following.

- Contract: if processing someone's personal data is necessary to fulfil the Colleges contractual obligations to them
- Legal obligation: if processing personal data is necessary to comply with a

common law or statutory obligation.

- Vital interests: if processing personal data is necessary to protect someone's life.
- Legitimate interests: when data is used in ways people would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- Public task: when processing is necessary for the College to perform a task in the public interest or for other official functions.

GDPR provides for special protection for children's personal data and the College will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16.

National Data Opt-Out

We review our data processing on an annual basis to assess if the national data opt-out applies.

If any data processing falls within scope of the National Data Opt-out, we use the Messaging Exchange for Social Care and Health (MESH) to check if any of our service users have opted out of their data being used for this purpose.

Right of Access to Information

Colleagues and students/clients may request details of personal information, which the College holds about them under the GDPR. If they would like a copy of the information held on them, they should contact the Data Protection Officer. In the Data Protection Officer's absence, requests from or relating to students and clients can be sent the Director of Communication, Information & Technology, and requests from colleagues can be made to the Human Resources department.

Information requests will normally be provided within one month. Where the request would involve a high volume of complex data to be collated, it may take up to 3-months to fulfil the request, and the individual requesting the data will be kept fully informed at all stages.

A request, which is manifestly unfounded or excessive, may be refused - the person concerned will then be informed of their right to contest this decision with the supervisory authority (the ICO).

If a colleagues or student/client believes that any information held on them is incorrect or incomplete, then they should write to or email the Data Protection Officer as soon as possible. The College will promptly correct any information found to be incorrect.

All other requests for access information should be made through the Data Protection

Officer.

Photographs and Videos

Images of colleagues and students/clients may be captured at appropriate times and as part of educational activities for use in college only.

Unless prior consent for staff or students has been given, the College shall not utilise such images for publication or communication to external sources.

It is the College's policy that external parties may not capture images of staff or students during such activities without prior consent.

CCTV

The College owns and operates a CCTV network for the purposes of crime prevention and detection and Safeguarding.

When a data subject can be identified, images will be processed as personal data.

Refer to the CCTV Policy for further details.

Privacy Impact Assessments

Where the college is undertaking a project which requires the processing of personal data it may be necessary for a Privacy Impact Assessment (PIA) to be completed. Where it is deemed that a PIA is required, form HR67 – Privacy Impact Assessment should be completed in these instances.

If you are unsure whether a PIA is required you should refer to the Data Protection Officer or consult the HR67, which provides a list of probing questions to enable a decision to be made.

Data Breaches

The Data Protection Officer should be notified immediately whenever there is a breach in the collection or processing of personal or sensitive data. The Data Protection Officer will review the breach and, if it is deemed to have a *significant adverse effect* on an individual's right or freedom, the individual(s) concerned will notified within 72 hours and the ICO will be notified without unnecessary delay.

A breach could include:

- loss or theft of hard copy notes, USB drives, computers, or mobile devices

- an unauthorised person gaining access to a laptop, email account or computer network.
- sending an email with personal data to the wrong person
- release of data to a third party without gaining prior consent
- a disgruntled employee copying a list of contacts for their personal use.
- sensitive documentation left on an unsecured desk.
- failure to lock a computer screen when not at your desk.
- a break-in at the office where personnel files are kept in unlocked storage.

Secure Destruction

When data held in accordance with this policy is destroyed, it will be destroyed securely in accordance with best practice at the time of destruction and a destruction notice will be provided.

Retention of Data

The College may retain data for differing periods and for different purposes as required by law.

The College may store some data such as registers, photographs, exam results, books, and works etc. indefinitely in its archives.

Refer to the Retention Policy and Schedule for further details.

Status of this Policy

The Policy does not form part of the formal contract of employment, but it is a condition of employment that staff will abide by the rules and policies made by Derwen College from time to time. Any failure to follow the Data Protection Policy may lead to disciplinary action up to and including summary dismissal.