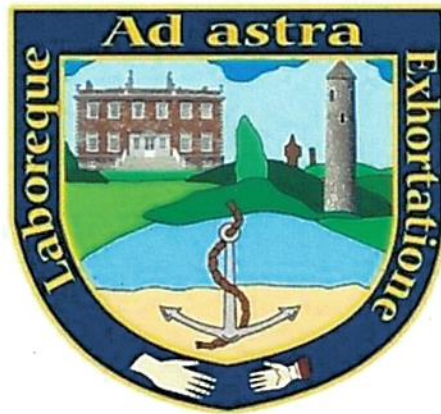


Data Protection Policy

DONABATE COMMUNITY COLLEGE

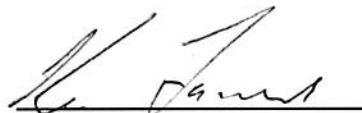


This Policy is to be reviewed by the Board of Management every two years.

This Policy was agreed on:

30/9/25.

Signature:



(Chairperson to the Board of Management)

Donabate Community College

Donabate Community College is a post primary college, which opened in August 2008 under the Patronage of Dublin and Dun Laoghaire Education and Training Board (DDLETB). The college is co-educational and aspires towards excellence in a caring and supportive environment. The Board of Management is committed to the successful implementation of recent legislation, in particular the Education Act (1998), the Education (Welfare) Act (2000) and the Equal Status Act (2000). The Board fully subscribes to the principles of partnership, accountability, transparency, inclusion and respect for diversity, parental choice and equality.

College Mission

The Board of Management will promote Excellence. Our aim will be to create, with the assistance of parents/guardians, responsible citizens with pride in their community. The development of the whole person will be based on personal responsibility, inter dependence, respect for people and respect for property. Our college will seek to instil integrity, value discipline and punctuality and facilitate the best in academic and non-academic areas. We will value our culture, our tradition, be inclusive of religious beliefs and will seek to be a caring and compassionate community where justice and truth will be the central elements.

Policy Review and Ratification

Donabate Community College is committed to ongoing policy review to ensure clarity, relevance, and compliance with current legislation and best practices. Where amendments to a policy are of a minor or administrative nature and do not alter its overall meaning, purpose, or intent, the school may proceed to seek ratification from the Board of Management without further consultation with stakeholders. However, where substantive changes are proposed that impact the policy's intent, scope, or application, appropriate consultation with relevant stakeholders will be undertaken before submission to the Board of Management for ratification.

Introduction

Donabate Community College is committed to protecting the personal data it holds about students, staff, parents/guardians, and others, in accordance with the General Data Protection Regulation (GDPR), the Data Protection Acts 1988–2018, and relevant Department of Education policies and circulars.

This policy explains how personal data must be collected, handled, and stored to meet the School's legal obligations, and to ensure that individuals' rights are protected.

Scope and Purpose

This Policy applies to all personal data processed by or on behalf of the School, including but not limited to:

- Student records (enrolment, attendance, assessments, special educational needs, health data, safeguarding records)
- Staff records (recruitment, payroll, performance management, occupational health, training)
- Parent/guardian and emergency contact information
- Visitors and external contractors
- Digital and CCTV records, photographs, video recordings, and other media
- Electronic systems (e.g. Vsware, School emails, cloud storage, learning management systems, etc.)

The purposes of data processing include (but are not limited to):

- Provision of education, pastoral care and support services
- School administration, enrolment and attendance monitoring
- Child safeguarding and welfare
- Meeting special educational needs and health supports

- Compliance with statutory obligations (e.g. Education (Welfare) Act, Child Protection legislation, employment law, Department of Education circulars)
- Communication with parents, guardians, students and staff
- Reporting and accountability to the Department of Education and other authorities
- Health and safety, CCTV, security, emergency planning
- Staff recruitment, payroll, occupational health, performance review and human resources

As required by GDPR and Irish law, we will only process personal data that is adequate, relevant and limited to what is necessary for the purposes for which it is processed (“data minimisation”), and we will retain it only for as long as necessary (“storage limitation”).

Legal Basis for Processing

The School processes personal data under one or more of the following lawful bases:

1. **Consent** — where the individual (or their parent/guardian) has given explicit consent to the processing of personal data for one or more specific purposes. Consent will be freely given, specific, informed and unambiguous, and may be withdrawn at any time.
2. **Contractual necessity** — where the processing is necessary for a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g. staff employment contracts, learner contracts).
3. **Legal obligation** — where the School has a statutory duty to process personal data (e.g. under the Education (Welfare) Act, Child Protection legislation, employment law, health & safety legislation).
4. **Public interest / official authority / vital interests** — where the processing is necessary for carrying out tasks in the public interest or exercising official authority vested in the School or the Education and Training Board, or to protect someone's vital interests (for instance, safeguarding children or responding to medical emergencies).
5. **Legitimate interests** — where processing is necessary for the School’s legitimate interests or the legitimate interests of a third party, provided that such interests are not

overridden by the interests or fundamental rights and freedoms of the data subject. Any legitimate interest basis must be documented and regularly reviewed.

Where special category personal data is processed (for example, health data, special educational needs, child protection records), an additional lawful basis is required under GDPR Article 9, such as:

- explicit consent, or
- necessary for reasons of substantial public interest,
- necessary for the provision of health or social care,
- necessary to protect vital interests,
- or other lawful bases as provided for in Irish law (for example, the Education for Persons with Special Educational Needs Act).

Processing of child protection and safeguarding data, or psychological and counselling records, may also rely on legal obligations and vital interests, given the duty of care owed by the School to students.

Data Protection Principles

All personal data processed by the School will be handled in accordance with the GDPR data protection principles:

1. **Lawfulness, fairness and transparency** — data will be processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. **Purpose limitation** — data will be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
3. **Data minimisation** — data collected will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy** — data will be accurate and, where necessary, kept up to date. Reasonable steps will be taken to erase or rectify inaccurate data without delay.

5. **Storage limitation** — personal data will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.
6. **Integrity and confidentiality** — data will be 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.
7. **Accountability** — the School is responsible for, and must be able to demonstrate, compliance with all of the above principles.

Roles and Responsibilities

Data Controller

Donabate Community College (board of management, principal, and ultimately the Education and Training Board) is the data controller for all processing of personal data.

Data Protection Officer (DPO)

For schools under the remit of an Education and Training Board (ETB), such as Donabate Community College, the **Dublin & Dún Laoghaire Education and Training Board (DDLETB)** has appointed a central Data Protection Officer (DPO) who acts on behalf of its schools and centres.

Contact details for the DDLETB DPO

- **Email:** dataprotection@ddletb.ie
- **Telephone:** 01-4529600

The DPO is responsible for:

- advising the ETB and its schools on compliance with GDPR and the Data Protection Acts,

- monitoring data protection practices across the ETB and its schools,
- coordinating or advising on data protection impact assessments (DPIAs) where required,
- coordinating data protection training and awareness for staff, and
- acting as the main point of contact for data subjects and the Data Protection Commission.

Day-to-day responsibility for ensuring compliance with data protection law within Donabate Community College rests with the Principal and staff, under the authority of the Board of Management, while the DPO provides independent oversight and expert advice.

In line with Department of Education practice, the ETB DPO liaises with the Department's Data Protection Unit as required, particularly where data sharing or formal reporting obligations are involved.

Staff Responsibilities

All staff (teaching, administrative, support, contractors) who process personal data on behalf of the School must:

- Familiarise themselves with this Data Protection Policy and any associated procedures and guidance.
- Ensure that personal data is accessed only where there is a clear business need, and only processes for the minimum time necessary.
- Use secure methods to store or transmit personal data (e.g. encrypted devices, password-protected files, secure cloud services, locked filing cabinets).
- Ensure that personal data is not disclosed to unauthorised persons, either within or outside the School.
- Report any suspected or actual personal data breach immediately to the DPO or principal.
- Cooperate with any review or audit of data protection practices within the School or by external bodies.

The School provides regular training and guidance for staff on data protection, including on new issues (remote learning, online platforms, cloud services, mobile devices, social media, etc.).

Privacy Notices

- The School will provide clear, accessible privacy notices to data subjects (or their parents/guardians) at or before the time personal data is collected, whether directly from data subjects or from other sources.
- Privacy notices will specify the purposes of processing, the lawful basis for processing, the categories of data being collected, recipients or categories of recipients of the personal data, retention periods, rights of the data subject (including the right of access, rectification, erasure, restriction, objection, data portability and the right to withdraw consent), and the contact details of the School's DPO.

These notices will be consistent with Department of Education / Department of Further & Higher Education "GDPR Privacy Notices" and public sector best practice, and will be kept under review. (gov.ie)

Data Subject Rights

The School recognises and respects the rights of data subjects under the GDPR and the Data Protection Acts. These rights include:

- Right to be informed (see privacy notices)
- Right of access (Subject Access Requests)
- Right to rectification of inaccurate or incomplete personal data
- Right to erasure ("right to be forgotten") in certain circumstances
- Right to restrict processing
- Right to data portability
- Right to object to processing, including for direct marketing or profiling
- Rights in relation to automated decision-making and profiling

The School will respond to all valid data subject requests within the statutory deadlines, and will have a published procedure for handling Subject Access Requests or other rights-based requests. (gov.ie)

Data Security and Confidentiality

Physical Security

- Personal data in physical (paper) form shall be kept in secure, access-controlled environments (locked filing cabinets or offices), and access shall be restricted only to authorised persons.
- Offices and filing rooms will be locked when unattended, and visitors will be supervised or escorted.

Technical Security

- Digital personal data must be stored securely: this means using strong passwords, regular password changes, encryption of portable devices, secure cloud services, up-to-date antivirus and patching, firewalls, and secure backups.
- Access to digital systems will be role-based and limited to those with a legitimate need. Login credentials will not be shared.
- When sending personal data electronically (especially by email or file transfer), encryption or secure file transfer mechanisms must be used where appropriate, particularly for sensitive or special category personal data.

Data Minimisation and Anonymisation

- Wherever possible, personal data will be pseudonymised or anonymised if full personal identifiers are not necessary for the immediate task.
- Personal data will only be kept in identifiable form for as long as strictly necessary; once it is no longer required, it should be archived or securely destroyed.

Data Retention and Secure Disposal

- The School will maintain a records retention schedule, specifying retention periods for different categories of personal data, consistent with Department of Education guidance and any statutory or regulatory obligations.
- Once personal data is no longer required, it will be securely disposed of: paper records should be shredded, electronic records should be deleted or securely wiped, and backups securely overwritten or destroyed.
- Special category data and safeguarding files should be disposed of with additional safeguards and in accordance with relevant legislation and department guidance.

Breach Notification

- The School will maintain a data breach response plan, which includes procedures for detecting, investigating and reporting data breaches.
- Where a personal data breach occurs that is likely to result in a risk to individuals' rights and freedoms, the School will notify the Data Protection Commission without undue delay, and where feasible within 72 hours of becoming aware of it.
- Where a breach is likely to result in a high risk to individuals, the School will also communicate with those individuals without undue delay.
- All staff must report suspected or actual data breaches promptly to the DPO or Principal, who will coordinate the response.

Data Sharing and Third Parties

- Personal data will not be shared with third parties unless there is a lawful basis, and sharing is necessary, proportionate and secure.
- Any sharing of personal data with external bodies (e.g. other schools, Department of Education, TUSLA, health services, examination bodies, contractors, cloud providers) will take place under a written data sharing agreement or contract, setting out the purpose of sharing, the responsibilities of both parties, security measures, confidentiality, and retention or return of the data.

- The School will ensure that third-party processors comply with GDPR requirements through appropriate contractual clauses and oversight.
- Transfers of personal data outside the European Economic Area will only take place where adequate safeguards are in place (e.g. standard contractual clauses, adequacy decision, or explicit consent).

CCTV, Photography and Video Recording

- The School operates CCTV and may capture photographic or video images of students, staff and visitors. These activities are governed by specific policies (e.g. a CCTV policy, an Acceptable Use Policy, and parental consent for photographs/video recordings).
- Notices will be placed where CCTV is active, and individuals will be informed about the purpose of CCTV recording, the retention period, and who to contact about access or objections.
- Use of photographs or videos for school publicity, social media, yearbooks or websites will require consent from parents/guardians (or students themselves, if they are of sufficient age and understanding), except where images are captured incidentally in public or school events and used in a way that does not identify the individual or invade privacy.

Staff Training and Awareness

- The School provides regular training, updates, and guidance for all staff on data protection, including:
 - GDPR and data protection legislation
 - The School's Data Protection Policy and associated procedures
 - Security best practice for physical and digital data
 - Handling personal data, responding to subject access requests, and reporting breaches
 - Specific issues such as remote learning, cloud services, mobile devices, online platforms, social media use, data retention and disposal

- Staff will be required to confirm that they have read, understood and will comply with the School's data protection policies and procedures.

Data Protection Impact Assessments (DPIAs)

- The School will conduct Data Protection Impact Assessments where required, particularly for new or substantially changed processes, systems or technologies that are likely to result in a high risk to individual rights and freedoms (for example, new CCTV systems, large-scale use of student tracking, new cloud-based learning management systems, new occupational health services, remote learning platforms, etc.).
- DPIAs will include: a description of processing, assessment of necessity and proportionality, assessment of risk to individuals, measures to mitigate those risks, and will be reviewed regularly.

Monitoring, Review and Governance

- Compliance with this policy and associated data protection procedures will be monitored regularly. The School may conduct audits, reviews or internal inspections of records management, access controls, staff compliance, breach reporting and retention schedules.
- The Policy will be reviewed at least annually or more frequently if required by legislative changes, new Department of Education circulars or guidance, or following a data breach or audit.
- Any substantial changes to this policy will be approved by the Board of Management.

Contact and Complaints

- If any individual has questions about this policy or how their personal data is processed, they should contact the School's Data Protection Officer.

- Data subjects have the right to make a complaint to the Data Protection Commission if they believe that Donabate Community College has not complied with its obligations under GDPR or the Data Protection Acts.

Appendix: Retention Schedule

Category of Data	Retention Period
Student enrolment records	Duration of enrolment + 7 years
Student attendance records	7 years after leaving
Examination results and assessments	7 years after leaving
Special educational needs files	Until end of school involvement + 10 years, or as required by law
Child protection & safeguarding records	Indefinitely or until transferred to adult services (in line with legislation and TUSLA guidance)
Staff personnel records	Duration of employment + 7 years
Payroll, pensions, financial records	7 years after ceasing employment
CCTV recordings	No more than 30 days unless retained for a specific incident
Visitor logs and gate security records	6 months
Photographs/videos used for publicity	Until consent is withdrawn or ceases to be relevant, then securely destroyed