



etbi
Education & Training
Boards Ireland
*Bord Oideachais &
Oiliúna Éireann*

Broadmeadow Community

National School,

Rathbeale Road,

Swords,

Co. Dublin

<https://broadmeadowcns.ie>

broadmeadowcns@ddletb.ie

Roll Number: 20529J

ACCESS TO RECORDS AND DATA PROTECTION POLICY

BROADMEADOW COMMUNITY NATIONAL SCHOOL



2025/2026

Principal: Miss J. Robinson

The Principal of Miss Jennifer Robinson is responsible for the implementation of this Access to Records and Data Protection Policy.

Introduction

At Broadmeadow CNS we take the storing and sharing of data very seriously and ensure that all regulations and legislation are in place and followed to protect you in the best way possible. The Data Protection Act, 1988, and the Data Protection (Amendment) Act, 2018, safeguard the privacy rights of individuals with regard to personal data i.e. data relating to them which is held on computer files or in manual files which are structured or searchable by reference to individuals.

This Data Protection Policy applies to the **personal data** held by the Board of Management /ETB of Broadmeadow CNS which is protected by the Data Protection Acts 1988 to 2018 and the EU General Data Personal Regulation (GDPR).

This policy applies to all school staff, the Board of Management/ETB, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation.

Rationale

This policy sets out what data will be collected, how personal data will be stored, managed and protected by Broadmeadow CNS and DDLETB. A policy on data protection and record keeping is necessary to ensure that the school has proper procedures in place in relation to accountability and transparency. It is good practice to record pupil progress so as to identify learning needs and ensure that there is consistency and continuity where there are changes of personnel within the school and Board of Management.

This policy ensures that Broadmeadow CNS complies with legislation such as the following:

- Section 9(a) of the Education Act, 1998
- Section 20 of the Education (Welfare) Act, 2000
- Section 20 (5) of the Education (Welfare) Act, 2000
- Section 21 of the Education (Welfare) Act, 2000
- Section 28 of the Education (Welfare) Act, 2000
- Section 14 of the Education for Persons with Special Educational needs Act, 2004
- Freedom of Information Act 1997
- Section 26(4) of the Health Act, 1947
- Children First Act, 2015

DDLETB Data Processing Policy

As Broadmeadow CNS is managed by the Patron of DDLETB, the data processing policies are underwritten by policy and procedure created for DDLETB. All copies of the Data Protection Policies for DDLETB can be found at

<https://www.ddletb.ie/corporate/corporate-about-us/publications/publications-policies/>

Broadmeadow CNS Definition of Data Protection

In order to properly understand the school's obligations at Broadmeadow CNS, there are some key terms which should be understood by all:

Data means information in a form that can be processed. It includes both *automated data* (e.g. electronic data) and *manual data*. *Automated data* means any information on computer, or information recorded with the intention that it be *processed* by computer. *Manual data* means information that is kept/recorded as part of a *relevant filing system* or with the intention that it form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.

Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller i.e. the school.

Sensitive Personal Data refers to *Personal Data* regarding a person's

- racial or ethnic origin, political opinions or religious or philosophical beliefs
- membership of a trade union
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence or
- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

Data Controller for the purpose of this policy is the Board of Management at Broadmeadow CNS.

Data Protection Principals

The school/ETB are a *data controller of personal data* relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the school is obliged to comply with the principles of data protection set out in the Data Protection 2018 which can be summarised as follows:

The Seven Key Principles of Data Protection (Ireland, 2018)

- **Lawfulness, Fairness & Transparency**

Data must be processed lawfully (with a valid legal basis such as consent, contract, or legal obligation).

Processing must be fair and transparent – individuals must be told how their data is being used.

- **Purpose Limitation**

Data must only be collected for specific, explicit, and legitimate purposes.

It cannot be reused for incompatible purposes.

- **Data Minimisation**

Only collect data that is adequate, relevant, and limited to what is necessary for the stated purpose.

- **Accuracy**

Personal data must be accurate and kept up to date.
Inaccurate data must be corrected or erased without delay.

- **Storage Limitation**

Data should not be kept longer than necessary.
Retention policies should define how long data is stored.

- **Integrity & Confidentiality (Security)**

Personal data must be processed securely.

Appropriate technical and organisational measures (e.g., encryption, access controls) should protect against unauthorised access, loss, or damage.

- **Accountability**

Organisations must be able to demonstrate compliance with all the above principles.

This means keeping records, carrying out Data Protection Impact Assessments (DPIAs), appointing Data Protection Officers (DPOs) where required, etc

Legal Principals

Implementation of this policy takes into account the school's other legal obligations and responsibilities. Some of these are directly relevant to data protection. **For example:**

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education if requested.
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School.
- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring.
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day.
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)

- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers (“SENOs”)) such information as the Council may from time to time reasonably request.
- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be “personal data” as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body.
- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection.
- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationship to School Ethos

Broadmeadow CNS seeks to:

- Enable each student to develop their full potential
- Provide a safe and secure environment for learning
- Promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society.

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us. The school wishes to achieve these aims/missions while fully respecting individuals’ rights to privacy and rights under the Data Protection Acts.

Data Collection and Management

Personal Data Collection

The Personal Data records held by the school **may** include:

Staff Data

Categories of staff data: As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details, PPS number, car details (Transportation of children with relevant insurance)
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

Purposes: Staff records are kept for the purposes of:

- The management and administration of school business (now and in the future)
- To facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- To facilitate pension payments in the future.
- Human resources management.
- Recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- To enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)
- To enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies.
- For compliance with legislation relevant to the school.

Location:

In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Any online data will be password secured. Some data will also be stored by DDLETB as the employer and can be shared between the school and employer.

Security:

Identify the format in which these records are kept e.g. manual record (personal file within a *relevant filing system*), computer record (database) or both. [Describe applicable security measures, e.g. locks, padlocks, password protection, firewall software, adequate levels of encryption etc.]

Student Data

Categories of student data: These **may** include:

Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:

- Name, address and contact details, PPS number.
- Date and place of birth.
- Names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
- Religious belief.
- Racial or ethnic origin.
- Membership of the Traveller community, where relevant.
- Whether they (or their parents) are medical card holders.
- Whether English is the student's first language and/or whether the student requires English language support.
- Any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply.
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student.
- Psychological, psychiatric and/or medical assessments.
- Attendance records.
- Photographs and recorded images of students (including at school events and noting achievements). See the template "Guidance on Taking and Using Images of Children in Schools"
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports.
- Records of significant achievements.
- Whether the student is repeating the Leaving Certificate.
- Whether the student is exempt from studying Irish.
- Records of disciplinary issues/investigations and/or sanctions imposed.
- Garda vetting outcome record (where the student is engaged in work experience organised with or through the school/ETB which requires that they be Garda vetted)
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

Purposes: The purposes for keeping student records are:

- To enable each student to develop to their full potential.
- To comply with legislative or administrative requirements.
- To ensure that eligible students can benefit from the relevant additional teaching or financial supports.
- To support the provision of religious instruction.
- To enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events etc.
- To meet the educational, social, physical and emotional requirements of the student.
- Photographs and recorded images of students are taken to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the school's "Guidance for Taking and Using Images of Pupils in Schools" (see template)
- To ensure that the student meets the school's admission criteria.
- To ensure that students meet the minimum age requirements for their course,
- To ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities.
- To furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other Schools etc. in compliance with law and directions issued by government departments.
- To furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/ references to third-level educational institutions and/or prospective employers.
- In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the School will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.

Location:

In a secure, locked filing cabinet that only personnel who are authorised to use the data can access.

Aladdin School online system is used to store and communicate data and information between families and school.

ESINET- POD System to store and communicate data between the Department of Education and School

Security:

Identify the format in which these records are kept e.g. manual record (personal file within a *relevant filing system*), computer record (database) or both. [Describe applicable security measures, e.g. locks, padlocks, password protection, firewall software, adequate levels of encryption etc.].

Password protection and encryptions as per Aladdin, Department and DDLETB guidelines.

Board of Management Data

Categories of board of management data: These may include:

- Name, address and contact details of each member of the board of management (including former members of the board of management)
- Records in relation to appointments to the Board.
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals.

Purposes:

To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.

Location:

In a secure, locked filing cabinet and that only personnel who are authorised to use the data can access it. Employees are required to maintain the confidentiality of any data to which they have access. Any online data will be password secured.

Security:

Identify the format in which these records are kept e.g. manual record (personal file within a *relevant filing system*), computer record (database) or both. [Describe applicable security measures, e.g. locks, padlocks, password protection, firewall software, adequate levels of encryption etc.]

Other records:

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive)

Creditors

Categories of data:

The school may hold some or all of the following information about creditors (some of whom are self-employed individuals):

- Name
- Address
- Contact details
- PPS number
- Tax details
- Bank details and
- Amount paid.

Purposes:

This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

Location:

In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Any online data will be password secured.

Security:

Identify the format in which these records are kept e.g. manual record (personal file within a *relevant filing system*), computer record (database) or both. [Describe applicable security measures, e.g. locks, padlocks, password protection, firewall software, adequate levels of encryption etc.]

Charity Tax-Back Forms**Categories of data:**

The school may hold some or all of the following information about creditors (some of whom are self-employed individuals):

- Name
- Address
- Contact details
- PPS number
- Tax rate
- Signature
- Gross amount for donation

Purposes:

Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the case of audit by the Revenue Commissioners.

Location:

In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Any online data will be password secured.

Security:

Identify the format in which these records are kept e.g. manual record (personal file within a *relevant filing system*), computer record (database) or both. [Describe applicable security measures, e.g. locks, padlocks, password protection, firewall software, adequate levels of encryption etc.]

CCTV images/recordings

Categories:

CCTV is installed in some schools, externally i.e. perimeter walls/fencing and internally as detailed in the CCTV Policy. These CCTV systems may record images of staff, students and members of the public who visit the premises.

Purposes:

Safety and security of staff, students and visitors and to safeguard school property and equipment.

Location:

Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is located in <state location>e.g. the Principal's office or in the reception office of school.

Security:

Access to images/recordings is restricted to <state authorised person> e.g. the principal & deputy principal of each school. Tapes, DVDs, hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

Examination Results

Categories:

The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual, continuous assessment and mock-examinations results.

Purposes:

The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

Location:

In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Security:

Identify the format in which these records are kept, e.g. manual record (personal file within a *relevant filing system*), computer record (database) or both. [Describe applicable security measures, e.g. locks, padlocks, password protection, firewall software, adequate levels of encryption etc.]

Links to Curriculum and Policies

At Broadmeadow CNS, our school policies need to be consistent with one another, within the framework of the overall School Plan. Relevant school policies already in place or being developed or reviewed, shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

- Child Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Electronic Devices & Mobile Phone Policy
- Admissions/Enrolment Policy
- CCTV Policy
- Substance Use / Misuse Policy
- ICT Acceptable Usage Policy
- SPHE Plan

Processing Data

Data in this school will be processed in line with the data subjects' rights and also in line with DDLETB Policy and Procedure located at;

<https://www.ddletb.ie/corporate/corporate-about-us/publications/publications-policies/>

Data subjects have a right to:

- Request access to any data held about them by a data controller.
- Prevent the processing of their data for direct-marketing purposes.
- Ask to have inaccurate data amended.
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Retention of Data

The following sets out the length of time that data will be held in storage in Broadmeadow CNS:

Pupil records	Retention Periods
Enrolment forms	Hold until pupil is 25 years old
Test results – standardised	Hold until pupil is 25 years old
Pupil profile / class handover booklet	Retained from J1 to 6 th class and then destroyed
Psychological assessments etc.	Never destroy
SEN files / IEPs	Never destroy
Accident reports	Never destroy
Disciplinary notes	Never destroy
Child protection reports / records	Never destroy
S.29 appeals	Never destroy
School register / roll books	Indefinitely
Staff records	Retention Periods
Contract of employment	Keep for length of employment + 7 years
Copy of PTAF	
Teaching council registration	6 years to make a claim against the school plus 1 year for proceedings to be served on school)
Vetting records	
Certificates for course attendance	
Doctors certificates for illness	
Accident / Injury at work reports	
Interview Records	Retention Periods

Interview board Marking scheme Board of Management notes	18 months from close of competition plus 6 months in case Equality Tribunal needs to inform school that a claim is being taken
BoM Records	Retention Periods
BOM agenda and minutes CCTV recordings	Indefinitely 28 days normally. In the event of criminal investigation – as long as is necessary
Payroll and taxation	Revenue require a 6-year period after the end of the tax year
Invoices / receipts	Retain for 7 years
Audited accounts	Indefinitely

Dealing with Data Access Requests

Section 3 access request

Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether the school holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 21 days. The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

Section 4 access request

Individuals are entitled to a copy of their personal data on written request.

- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- Request must be responded to within 40 days.
- Fee may apply but cannot exceed €6.35.
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where

it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

Requests of Data

- All data requests must be completed through DDLETB using the appropriate template for GDPR or Freedom of Information requests. All requests must be placed in writing directly to the school Principal who will then forward on the appropriate details or request forms for completion.
- Please allow the appropriate level of time for a response for all requests through our corporative services team.

Providing Information Via Telephone

At Broadmeadow CNS, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the school over the phone. In particular the employee should:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information.
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified.
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Implementation, Roles and Responsibilities

In our school the board of management is the data controller and the principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

The following personnel have responsibility for implementing the Data Protection Policy:

Name	Responsibility
Board of Management	Data Controller
Principal	Implementation of Policy
Teaching Staff	Awareness and implementation of Policy Confidentiality

	If a parent requests GDPR or Freedom of Information requests these must be issued to the Principal. Security, Encryption and Confidentiality
Administrative Staff	Security, Encryption and Confidentiality
IT Personnel	Security, Encryption and Confidentiality

Ratification and Communication

When the Data Protection Policy has been ratified by the Board of Management, it becomes the school's agreed Data Protection Policy. It should then be dated and circulated within the school community. The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on students, staff and others in the school community.

Parents/guardians and students should be informed of the Data Protection Policy from the time of enrolment of the student e.g. by including the Data Protection Policy as part of the Enrolment Pack, by either enclosing it or incorporating it as an appendix to the enrolment form.

Monitoring and Implementation of Policy

The implementation of the policy shall be monitored by the Principal and a sub-committee of the Board of Management.

This policy is implemented alongside all DDLETB Data Protection Policies located at;

<https://www.ddletb.ie/corporate/corporate-about-us/publications/publications-policies/>

Reviewing and Evaluating the Policy

The policy should be reviewed and evaluated at certain pre-determined times and as necessary. On-going review and evaluation should take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or the NEWB), legislation and feedback from parents/guardians, students, school staff and others. The policy should be revised as necessary in the light of such review and evaluation and within the framework of school planning.

Signed: B.Manton

For and behalf of board of management

Date: 06/10/26

Signed: J Robinson

Principal

Date: 06/10/26