

## **Danu Community Special School**

### **Data Protection Policy**

#### **Introduction**

This policy was formulated by the Management of Danu Community Special School (Danu CSS). This policy is in keeping with General Data Protection Regulations (GDPR), May 2018 and DDLETB's Data Protection Guidelines. The purpose of the policy is to identify the data and records required and retained by the school and to ensure confidentiality and manageable procedures in relation to access to such records by parents and stake holders. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school. The policy applies to all school staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school).

#### **Rationale**

GDPR applies to the keeping and processing of Personal Data, both in hard copy and electronic form. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to school staff, and to inform staff, students and their parents/guardians how their data will be treated. 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.

A policy must be put in place to ensure a school complies with legislation such as:

- 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
- 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 (EPSEN) 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 ensure all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) 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).
- The Employment Equality Acts 1998
- The Child Protection Procedures for Primary and Post Primary Schools 2017
- The Teaching Council Acts 2001-2015
- Safety, Health and Welfare at Work Act 2005

## **Aims/Objectives**

- To ensure the school complies with legislative requirements.
- To clarify the types of records maintained and the procedures relating to making them available to the relevant bodies.
- To put in place a proper recording and reporting framework on the educational progress of pupils.

- To establish clear guidelines on making these records available to parents and pupils over 18.
- To stipulate the length of time records and reports will be retained.

## **Data Controller**

DDLETB is the data controller. DDLETB oversees our Data Protection Policy and our Guidelines of Retention of Records. The Data Protection Officer (DPO) in DDLETB can be contacted for any data requests. The Principal assumes the function of data controller within the school and supervises the application of the Data Protection Act 2018 within the school.

## **Data Protection**

The school accepts that it owes each data subject (student, parent/guardian, teachers, SNAs and other staff members) a duty to ensure the protection and security of that data and has appropriate security measures in place to prevent “unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction”.

We will ensure that all data is:

- Accurate and kept up to date.
- Processed lawfully, fairly and in a transparent manner.
- Collected and processed for specific, explicit and legitimate purposes.
- Stored carefully and only for the recommended period of time.

## **Personal Data from the Data Subject (Child)**

This data is collected upon enrolment in Danu CSS. This data relates to personal details of the students such as:

- PPSN
- Name
- Address
- Date of birth
- Place of birth
- Parents/Guardians’ names and contact details
- Mother’s maiden name
- Gender
- Class
- Custodial orders/access
- Nature of SEN
- Ethnic origin
- Nationality
- Religious belief
- Medical details
- Dietary information

- Photographic Id
- Details of Professional Reports
- Enrolment Date

**The following documents are stored in each student's file**

- Personal details of the student
- Psychological Assessment Reports
- Multi- Disciplinary Team /Psychiatric Reports
- Court Order relating to Guardianship/Custody/Access or other family arrangements
- Information in relation to medical issues and health related conditions and /or Medical Assessments
- IEPs and School Reports
- Academic records, Assessment records, Individual Education Plans, Fortnightly Plans and End of Year School Reports
- Attendance Records
- Photograph/Media Permission
- Other Permission Forms
- Bullying Incident Records
- Incident Report Records
- Accident Report Forms

**Other data may be collected as the student progresses through the school such as**

- English as the student's first language and/or whether the student requires English language support
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student)
- Photographs and recorded images of students (including at school events and noting achievements). See Policy on Taking and Using of Photographs of Students in Danu CSS.
- Records of significant achievements
- Records of disciplinary issues/investigations and/or sanctions imposed
- 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)

**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/ SNA or financial supports

- to support comprehensive assessment
- 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 Policy on Taking and Using of Photographs of Students in Danu CSS.
- to ensure that the student meets the school's admission criteria
- 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 adult services

### **Storage and Security of Student Data**

Student records will be located in a secure, locked filing cabinet that only personnel who are authorised to use the data can access. **They may not be removed from school premises.** Day to day records of student's progress, reports and guidelines are kept in a file in the classroom. Hard copy records are kept in a students' personal file within a relevant filing system. More sensitive records are stored in a locked filing cabinet in the School office. Some personal information is also kept on a secure database that is password protected. Digital records such as student attendance records and PPS numbers are maintained on the POD system in line with DES Guidelines. Access will be by permission of the Principal or authorised personnel only. Attendance records are also kept on the school's secure database (Aladdin) and this is password protected.

Employees are required to maintain the confidentiality of any student data to which they have access.

### **Child Protection**

Child Protection reports are kept in a secure filing cabinet in a locked room. These files are only accessible by the Designed Liaison Person (DLP) and the Deputy Designated Liaison Person (DDLDP).

## **In relation to the Data Subject (Child), we share data with the following organisations:**

### **Aladdin**

This is an encrypted school administration database used by the school. They operate in line with current GDPR guidelines. Student details are stored on an online database. Aladdin is the MIS for Primary Schools and is the MIS recommended by the DES.

### **SeeSaw Ireland**

This is a digital portfolio tool supported by the Professional Development Service for Teachers used for distance learning between school and home. Class name and student full name is stored.

### **Department of Education and Skills (DES) and Primary Online Database (POD)**

We collect data to be transferred to the Department of Education and Skills via the Primary Online Database (POD) system as outlined in Circular 0050/2015 Fair Processing Notice to explain how the personal data of pupils in special schools on the POD will be recorded, processed and shared.

### **Psychological Assessments and other SEN reports**

Psychological Assessments are kept on file in a hard copy format in the Principal's office and shall not be removed. These are shared with outside agencies such as the Primary Care Team, NEPS, SENO & other agencies. Permission will always be sought from parents before transferring these documents.

### **National Council for Special Education (NCSE) & Special Educational Needs Organiser (SENO)**

We may contact the NCSE & SENO when submitting applications for enrolment, transport and other additional supports. All SEN applications pertaining to pupils are read and signed by the parents of the child, prior to the application being sent to the NCSE.

### **TUSLA Child and Family Agency**

Under the Children First Act 2015 and Child Protection Procedures for Primary and Post Primary Schools 2017, we seek advice from and/or make referrals to TUSLA if we suspect any form of child abuse or receive a disclosure of child abuse.

### **Education Welfare Officer (EWO) & National Educational Welfare Board (NEWB)**

In accordance with the Education Act 1998 & 2018, we liaise with the EWO/NEWB in relation to attendance, suspensions, and expulsions.

### **An Garda Síochána**

We may contact the Gardaí in relation to child protection issues and other criminal matters.

## **Health Service Executive (HSE)**

Occasionally, the HSE contacts us to seek data in relation to vaccination programmes or dental check-ups for children or similar public health issues. This is to enable the HSE to invite groups of children to participate in vaccination programmes or other public health initiatives. Parental permission is always sought before any vaccinations or testing takes place on the school grounds.

## **Data Transfer between Schools/Outside Agencies**

Written parental authorisation must be given by parents in the event of data being transferred to other schools. A letter or email requesting access to records must be received prior to transfer of data.

## **Personal Data from the Data Subject (Staff/ BOM)**

### **Staff Data**

The following data is kept for each staff member

- PPSN
- Name
- Address
- Date of birth
- Contact details and in the event of an emergency contact details
- Payroll number
- Attendance records
- Teaching council records
- Garda Vetting certificate
- Contracts
- Bank details (where necessary)
- Original records of application and promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, certificates, classes taught etc.)
- Details of any incident report or 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).
- Medmark Certificate

### **Security**

The records of staff members current and former are kept in hard copy and digital format in personal files and in digital format as on OnLine Claims System (OLCS) provided by Department of Education and Skills (DES). Hard copy files are retained in the Principal's Office. The Principal and DDLETB HR and IT Department only will have access to those files

that will contain information solely related to professional matters. Digital files are retained on the Principal's /Secretary's computer and are protected by password known only to IT Department in DDLETB and the Principal. Staff contact details are also stored on Aladdin.

### **Staff Incidents and Accident Reports**

All Incident Reports and Accident Reports will be kept safely in locked filing cabinets.

### **Staff Email**

All staff have access to a school email account. This is the only permitted email to be used on school devices. This is the only account that must be used regarding communicating school business.

### **Board Of Management**

The following data is kept for each BOM member

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

### **Purpose and Security**

The purpose to keeping these records is to enable the BOM to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions. Digital records are kept on Principal's secure encrypted computer and school server where only personnel who are authorised to use the data can access it. Hard copy records are kept in a BOM file within a relevant filing system. They are stored in a locked filing cabinet in the School office. BOM contact details are also stored on Aladdin.

### **Other Records**

Visitors sign a Visitor's sign in book providing their name and company details. Records relating to contacts with others such as Patron DDLETB, FIDO, banking, insurance companies, legal advice, buildings and lands etc. will be securely maintained in the manner appropriate to its origins e.g. paper correspondence or email as appropriate. The school will hold other records relating to individuals. The format in which these records will be kept are hard copy record (personal file within a relevant filing system), and/or computer record (database).

The school may hold some or all of the following information about creditors:

- Name
- Address
- Contact details
- Bank details and amount paid.



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. These are held in a secure, locked filing cabinet that only personnel who are authorised to use the data can access and may also be kept as a computer record on the Principal's or Secretary's secure encrypted computer that is password protected.

The school may hold the following data in relation to donors who have made charitable donations to the school:

- Name
- Address
- Contact details
- PPS number
- Tax rate
- Signature and
- The gross amount of the donation.

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. These records are held in a secure, locked filing cabinet that only personnel who are authorised to use the data can access and may also be kept as a computer record on the Principal's or Secretary's secure encrypted computer that is password protected.

The school may hold data on personal details e.g. name, address, PPSN, references for bus contractors, volunteers, student teachers and SNAs for work experience. Hard copy files are kept for students and SNAs for the current school year only. Hard copy files for volunteers are kept for the duration of the period spent volunteering in the school and for one year after completion. These records are held in a secure, locked filing cabinet that only personnel who are authorised to use the data can access and may also be kept as a computer record on the Principal's or Secretary's secure encrypted computer that is password protected.

### **Providing Information Over the Phone**

In our school, 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.

### **Providing Information Over Microsoft Teams Meetings**

In the event of working remotely from home and the necessity of remote virtual meetings to be held, the school will use Microsoft Teams to do so. Meetings are private and confidential and must be treated the same as with face to face meetings. Video imaging of employees during the meeting is necessary to protect the integrity of the meeting.

### **Data Retention**

Please see our Guidelines on Retention of Records.

### **Access to Records**

The following personnel will have access where relevant and appropriate to the data listed above:

- Parents/Guardians
- Past Pupils over 18
- Health Service Executive\TUSLA\NEWB
- Designated School Personnel
- Department of Education and Skills

### **Data Breaches**

The following are some examples of data breaches that can occur:

- Stolen Briefcase/bag – bags/briefcases containing any IEPs, etc.
- Wrong Email address – sending sensitive information by email to the wrong address
- Missing Packages – carrying around files on children – they could be left down, taken from a public place etc.

Staff are only required to access data on a “need to know” basis in order to carry out their job. It is now a Criminal Offence to intentionally access data you have no entitlement to see. Purposefully or knowingly destroying sensitive information belonging to the school in relation to children, planning or the smooth running of the school.

### **Sanctions as a Result of Data Breaches**

The loss of personal data is extremely serious. It can result in great distress for the data subjects involved. For the school, it can be disastrous, resulting in the imposition of large fines, damage to reputation and can lead to criminal prosecution of the school.

Due to this, any data breaches as a result of a staff member being careless or irresponsible may lead to disciplinary action up to and including dismissal. The school is bound to report any breaches of data to the Office of the Data Protection Commissioner.

Abuse of Data privileges can lead to serious disciplinary action, up to and including dismissal.

### **Links to Other Policies and to Curriculum Delivery**

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 Safeguarding Statement
- Anti-Bullying Policy
- Code of Behaviour
- Admissions and Participation Policy
- Intimate Care Policy
- Acceptable Use Policy

### **Success Criteria**

- Compliance with Data Protection Act May 2018
- Easy access to records
- Manageable storage of records
- Compliance with Danu CSS's Guidelines of Retention of Records
- Completion of the ETBI GDPR Training

### **Roles and Responsibilities**

The school staff, under the direction of the Principal will implement and monitor this policy. The Principal will ensure records are maintained and stored.

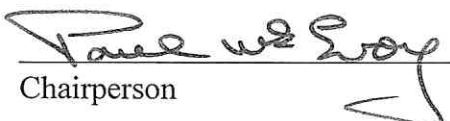
### **Review and Ratification**

This Data Protection Policy was ratified and communicated by the Board of Management on

24/6/20.

It is envisaged that the school will review this Data Protection Policy in June 2022 unless it needs to be amended prior to this time.

**Signed By**

  
Chairperson



Principal/Secretary Board of Management