Data Protection Policy

Introduction

This Data Protection Policy applies to the personal data held by Donabate/Portrane Educate Together ("DPETNS" or "the school") which is protected by the Data Protection Acts 1988 to 2018.

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) insofar as the measures under this Policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

Data Protection Principles

The school is 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 Acts 1988 and 2003 which can be summarised as follows:

- **Obtain and process Personal Data fairly**: Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. The information will be obtained and processed fairly.

- **Keep it only for one or more specified and explicit lawful purposes**: The School will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put.

- **Process it only in ways compatible with the purposes for which it was given initially**: Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

- **Keep Personal Data safe and secure**: Only those with a genuine reason for doing so may gain access to the information. Sensitive or 'Special Categories' of Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

- **Keep Personal Data accurate, complete and up-to-date**: Students, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date.

- **Ensure that it is adequate, relevant and not excessive**: Only the necessary amount of information required to provide an adequate service will be gathered and stored.

- **Retain it no longer than is necessary** for the specified purpose or purposes for which it was given: As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student as set out in the Data Retention Schedules set out at www.dataprotectionschools.ie.

- **Provide a copy of their personal data to any individual, on request**: Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

Definition of Data Protection Terms

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

Data means information in a form that can be processed. It includes both automated data (e.g. electronic data) and manual data.

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 natural person 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 or 'Special Categories' of 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.
- Biometric data (such as fingerprints)
- Genetic data

Data Controller for the purpose of this policy is the Board of Management, DPETNS.

Other Legal Obligations

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;
- 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);
- 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)

Personal Data

The Personal Data records held by the school is set out in the attached **Data Protection Schedule**.

Data Subject's Rights

Data in this school will be processed in line with the data subjects' rights.

Data subjects have a right to:

(a) Request access to any data held about them by a data controller
(b) Object to the processing of their personal data
(c) Prevent the processing of their data for direct-marketing purposes

(d) Ask to have inaccurate data amended

(e) Data subjects have the right to complain to the Data Protection Commissioner

(f) Data subjects have the right to be forgotten, or to require DPETNS to delete his or her personal data where that data is no longer needed for its original purpose, or where the processing is based on consent and the data subject withdraws that consent and no other lawful basis for the processing exists.

(g) Where DPETNS has disclosed personal data to third parties, the data subject has the right to request information about the identities of third parties to whom his or her personal data have been disclosed.

(h) Portability. A data subject may request a copy of his or her personal data in a commonly used machine-readable format, and to transfer it to another data controller.

Dealing with a Data Subject Access Request

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 30 days

* 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.

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.

Implementation arrangements, roles and responsibilities

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

Name	Responsibility
Board of Management:	Data Controller
Principal:	Implementation of Policy
Teaching Personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

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 and by a Privacy Notice on the school's website.

Monitoring the implementation of the policy

The implementation of the policy shall be monitored by the principal and a sub-committee of the board of management.

At least one annual report should be issued to the board of management to confirm that the actions/measures set down under the policy are being implemented.

The Records Retention Schedule for Donabate/Portrane ETNS consists of that set out by dataprotectionschools.ie and Appendix (1) – ***Additional Data Protection Schedule for DPETNS 2018***

Appendix (1) ADDITIONAL DATA PROTECTION SCHEDULE FOR DPETNS

Section 1 Data and the School Office

Data Collected	Legal basis/Purpose	Storage/Access
Aladdin	Aladdin is the school's official digital depository. A GDPR-compliant data processing agreement with Aladdin has been signed and is available on request.	
Family Directory Form	The data here is submitted on an annual basis to the school for the purposes of safety re dropping to school and collecting from school, access to children by parents and nominated-others, and updates parents permissions for various school protocols and medical-updates.	This data must be retained for the full duration of the child's life in the school. It is stored in a locked filing cabinet in the locked office. The data is properly disposed of when the child graduates.
Teacher/Employee Data	The school holds teachers, SNA and all employee data on the Aladdin, DES's OLCS system and in hardcopy-files. The data collected refers to contact details/ records of leave, records of contracts, records of teaching/employment-history and are all necessary for the governance of the school in keeping with BOM governance protocols. On a voluntary basis the teachers may also have stored their bank details (for the purposes of remuneration and refund of expenses) and car insurance details (for the purposes of complying with DES regulations regarding use of staff cars for school business) .	The Aladdin and OLCS systems are password protected. The hardcopy files are kept in locked cabinet in locked office. Records of contracts are kept for the duration of the teachers employment and a further 7 years beyond that.

Section 2 Data and Principal

OLCS system	The Principal is an authorised approver of all data held on the DES's OLCS system	This access is specifically passworded for Principal and Deputy Principal as approvers, and for the secretary only as data-inputter.

Section 3 Data and Parents

Data Collected	Rationale/Purpose	Storage/Access
Parent Teacher Association and associated parent groups.	The Parent Teacher Association may collect, on a voluntary basis, the names, addresses and contact details of volunteer members exclusively. Similarly for Catholic Parent Group/Book Rental Group etc	The Chairperson and Secretary of the PTA are to ensure that access to this databases/hardcopy is available only to the PTA and used exclusively for the purpose of PTA activity and no-other purpose. Similarly for other parent Groups.
Parents and other parents	At the beginning of each year parents are invited to be included in a class parent contact list. The list is shared only with those parents who have consented to be included in the list.	Other than this contact list the school does not share for any purpose any data from one parent to another (such as contact details etc) and does not authorise any parent to construct a communication channel between any parents if such is done with reference to school-business.

Section 4 Data and Teachers/SNAs (Each classroom/SEN room has a secure lockable cabinet for the purposes of storing sensitive data)

Teachers and Aladdin	Teachers may record, exclusively, Pupil progress report card, roll-call for attendance, relevant medical information and standardised test scores on Aladdin. No other pupil records should be stored on Aladdin.	Teachers should ensure not to divulge their Aladdin password to any other person, and passwords should not be stored by default on the class computer. Aladdin should be closed down when not in use, and when the room is unoccupied.

Teacher Generated Documents	Any documentation generated by a teacher, or shared to the teacher by a parent, that refers to issues of medical nature, assessment reports, care/child-protection concern , school attendance should be kept on the child's file in a locked filing cabinet.	Kept indefinitely by school principal.
Teachers and Class notes and Child Protection Notebooks	Throughout the year the teacher may keep a journal of incidents, reflections and observations as an aide memoire. Pseudonyms or Initials should be used when referring to a child. Should any of these memoires warrant any further attention under the school's child-safeguarding , anti-bullying or discipline procedure these matters should be brought to the Principal's attention who will then keep a formal record. Child Protection Notebooks are kept in a locked filing cabinet and are passed on to the class teacher the following year.	See anti bullying policy etc
Teaching/Learning data and ICT	Teachers shall ensure not to cause or facilitate the children in inputting any data to third-party sources that are personal or identifying. For such ICT programmes the teacher should establish a coded or school-generated identity that will be deleted and disposed of once the programme has been completed.	
Website and Social Media	The school's website and Facebook account have a prominent Privacy Statement.	No personal data for any person/child in the school community ever to be shared or posted.

Data and Board of Management

Data Collected	Rationale and Purpose	Storage/Access
The BOM hold responsibility for the governance of the school's GDPR		
The school, for the moment, is not required to appoint a data protection officer, but the BOM authorize the principal to function as an informal DPO while the BOM retains the governance liability.		
BOM Docs	The BOM documents are stored securely. Hard copies of the minutes are stored in a locked cabinet in a locked room.	The principal stores the BOM minutes in the locked filing cabinet in the locked office. Older minutes are stored in a locked room. These minutes are kept indefinitely.
BOM confidentialty	All BOM members are obliged to observe confidentiality about matters discussed at BOM, and any document distributed as part of BOM discussions should be returned at the end of the meeting and shredded. One copy of all BOM documents will be stored securely	
Staff Training	The BOM authorise the principal to direct all staff to conduct training and briefings on this GDPR on an initial and ongoing basis, and breaches of the GDPR will be dealt with under the school's Complaint and Grievance procedure	
Financial records	The financial records of the school are also to be treated as confidential and should only be disclosed to the school's authorised accountant.	The school's Financial records are stored in the locked office and annual finacial reports to be stored indefinitely.
The BOM will on an ongoing basis approve research projects, public relations exercises and access to the school by student-teachers TY and SNA persons etc which are of benefit to the	The principal will inform the parents of any such projects or placements as they occur.	When engaging in these projects the principal will ensure the highest ethical standards apply and that there is no potential harm (and indeed a particular educational gain) or

school and in keeping with its committment to its broader community.		exposure to the child from engaging in these projects.
SNAs	SNAs may keep a journal for recording of incidents, observations and reflections but these entries are understood as aide memoires. Any important or ongoing concern as recorded in this aide memoire should be brought to the principal for formal discussion and recording. The SNAs journal should be stored securely and handed to the Principal at the end of the school year and stored securely and indefinitely.	Formal records on school templates and NCSE templates recorded by the SNA should be handed to the school Principal for storing and archiving. These records are kept indefinitely.

Data and Other Agencies

Tusla and Tusla authorised services, Gardai, Revenue Commissioners Sepratment of Socila Protection, Applications on foot of court order	The school will comply fully with all requests from these statutory agencies.	
Family solicitors	Requests for school data from a family solicitor, whether via a parent, or independently delivered to the school, will be dealt with on a case by case and may involved legal advice or consultation with the national Data Protection Office.	
HSE and private health professionals	Any data requested by a HP can only be released with the explicit permission by the child's parent. The school keeps a record of any such data that has been shared	

	and is kept by the Principal in the 'files for Specific Children' (see above) in a locked cabinet in a secure location.	
Community Organisations	Community organisation are not allowed to collect data from children on their visits to the school, nor will the school facilitiate the sharing of any such data.	
Department of Education and Skills and DES officers	The DES is the Data Protection controller of the POD and OLCS systems, and are responsible for any breaches of this data. The school complies with any exposure of data to the school's Inspectorate that may arise during school evaluation (eg access to IEPs, teacher-folders, anti-bullying index, child safeguarding index etc.)	