Policy:	*Data Protection Policy*
Date:	*May 2021*
Date of next review:	*May 2023*

ENABLE IRELAND SANDYMOUNT SCHOOL

DATA PROTECTION POLICY

2021

DATA PROTECTION POLICY

Introductory Statement

The school's Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 to 2018 and the EU General Data Personal Regulation (GDPR) 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 the 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.

Enable Ireland Sandymount School operates a "**Privacy by Design**" method in relation to Data Protection. This means we plan carefully when gathering personal data so that we build in the data protection principles as integral elements of all data operations in advance. We audit the personal data we hold in order to:

1. Be able to provide access to individuals to their data
2. Ensure it is held securely
3. Document our data protection procedures
4. Enhance accountability and transparency

Data Protection Principles

The school BOM 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 BoM is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 to 2018 and GPDR 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. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. 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. All information is kept with the best interest of the individual in mind at all times.

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.

Consent: Where consent is the basis for provision of personal data, (e.g. data required for home/ school diary or online activities such as SeeSaw or any other school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes. Enable Ireland Sandymount School will require a clear, affirmative action e.g. ticking a box/ signing a document to indicate consent. Consent can be withdrawn by data subjects in these situations.

Keep Personal Data safe and secure: Only those with a genuine reason for doing so may gain access to the information. Sensitive 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. Once informed, the school will make all necessary changes to the relevant records. The Principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.

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. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.

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.

Scope

Purpose of the Policy: The Data Protection Acts 1988 and 2003 apply to the keeping and processing of *Personal Data*, both in manual 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.

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 school handles or processes their *Personal Data* in the course of their dealings with the school.

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*. *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 forms 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's BoM.

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.
- Genetic and biometric data

Data Controller for the purposes of this policy is the Board of Management of Enable Ireland Sandymount School.

Data subject is an individual who is the subject of the personal data

Data processing performing any operation or set of operations on data, including:

- obtaining, recording or keeping data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,

- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data

Data processor a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection legislation places responsibilities on such entities in relation to their processing of the data, for example Aladdin and text-A-Parent.

External Data Processors who provide services to Enable Ireland Sandymount School involving the processing of personal data are:

- Aladdin School Administration Software Package (1)
- HostingIreland.ie (school website domains and hosting) (2)
- Enable Ireland I.T. Department (server space, Microsoft Office 365 Cloud Hosting, mail server)
- Wiltshire Farm Foods
- FHM Accountants
- Zoom Video Conferencing (3)
- Seesaw (4)
- Instagram (5)
- Text-A-Parent (SMS service)

(1) Terms & Conditions: https://www.hostingireland.ie/termsandconditions.php
(2) Terms & Conditions: https://www.aladdin.ie/content/terms
(3) Terms of Service: https://web.seesaw.me/terms-of-service
(4) Terms & conditions: https://zoom.us/terms
GDPR: https://zoom.us/gdpr
(5) Terms & Conditions: https://www.instagram.com/about/legal/terms/before-january-19-2013/

Organisations we share data with:

- National Council for Special Education
- Health Service Executive
- DES: POD (Pupil On-line Database), OLCS (Online Claims System)
- Bus Éireann
- Tusla, Child & Family Agency

This is not an exhaustive list.

Data Protection Officer

Article 37 of the General Data Protection Regulations (effective 25th May 2018) makes it mandatory for data controllers and processors to designate a DPO in certain circumstances including, inter alia, where:
• the processing is carried out by a public authority or body (irrespective of what data is being processed).

Special Needs Schools have been identified as a category under the legislation that will require DPOs.

The GDPR also make reference to the designation of DPOs in other cases, i.e. where not mandatorily required, and in this regard the independent European data protection and privacy advisory body (the Art. 29 Working Party) encourages designation of a DPO on a voluntary basis when not specifically required.

If designating a DPO on a voluntary basis, the same requirements and responsibilities will apply to the position as if it had been made on a mandatory basis. An alternative approach, where not mandatorily required to have a DPO, would be to have an equivalent to a DPO but making clear that it is not a DPO designated for the purposes of the GDPR.
A DPO is not personally responsible for non-compliance with data protection requirements. Compliance remains the responsibility of the controller or processor. The DPO facilitates compliance with data protection laws.

This role has been appointed to the principal.

Role/Function of the DPO

The GDPR detail the following characteristics of the role:
• The DPO shall be designated on the basis of professional qualities and in particular expert knowledge of data protection law and practices.
• The controller and processor shall ensure that the DPO is involved properly and in a timely manner in all issues relating to the protection of personal data.
• The DPO must be supported by the controller and processor in the performance of its tasks (including being provided with the appropriate resources to carry out the tasks of the role and to maintain his/her expert knowledge (training) and access to personal data and processing information).
• The controller and processor must ensure that the DPO does not receive any instruction regarding the exercise of his/her tasks, including a prohibition on dismissal or penalisation by the controller or processor for performing his tasks.
• The DPO shall report directly to the highest management level of the controller or processor.
• Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under the GDPR.
• The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks
• The DPO shall in the performance of his/her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
• The DPO may fulfil other tasks and duties provided the controller / processor is satisfied that there is no conflict of interest (i.e. he/she should not be involved in determining the purpose and means of processing).
• The controller or processor must publish the DPO's contact details and communicate them to the ODPC. Professional qualities and expertise include:
• having an expertise in national and European data protection laws and practices including an in-depth knowledge of the GDPR;
• understanding of the processing operations;
• understanding of IT and data security;
• knowledge of the sector;
• ability to promote a data protection culture within the organisation.

The DPO shall have the ability to fulfil, at a minimum, the following tasks:

i. To inform and advise the controller/processor and the employees who carry out processing of their GDPR and other E.U. or domestic data protection provisions;
ii. To monitor compliance with the GDPR, other Union or domestic data protection provisions and with the controller/processor's data protection policies;
iii. Responsibility for awareness raising and training of staff involved in processing operations and responsibility for related audits;
iv. To provide advice where requested regarding the data protection impact assessment and monitor its performance
v. Cooperate with the ODPC;
vi. Act as the contact point for the ODPC on issues relating to processing, including where GDPR prior consultation obligations with the ODPC arise and to consult as appropriate with regard to any other matter.

The Principal as Data Protection Officer (DPO)

The Principal will ensure that the basic principles of data protection are explained to staff and parents/guardians. This will be done during staff induction, staff meetings and via the staff handbook.

The Principal will ensure that there are regular updates to data protection awareness, so that data protection is a "living" process aligned to the school's ethos and periodically check data held regarding accuracy

Personal Data Breach a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This means any compromise or loss of personal data, no matter how or where it occurs.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, Enable Ireland Sandymount School has a legal responsibility to comply with the Data Protection Acts, 1988 to2018 and the GPDR 2018.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

Enable Ireland Sandymount School takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the Principal and Board of Management to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and Board of Management.

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, if the situation arises.
- Where reports which have been carried out by professionals, apart from Enable Ireland Sandymount School staff, are on current pupil files; such reports are only passed to the Post Primary school following written permission having been sought and received from the parents of the said pupils.
- 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 characteristic spirit of the School (School's mission/vision/aims)

Enable Ireland Sandymount School 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.

Personal Data

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

A. Staff records:

(a) 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.
- Name and contact details of next-of-kin in case of emergency.
- 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 and Children's First Act 2015).

(b) 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 and for compliance with legislation relevant to the school.

(c) Location and Security:

1. Manual records are kept in a secure, locked filing cabinet in a locked administration office 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.
2. Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office. School has burglar alarm set in closed hours.

B. *Student records:*

(a) 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) are managed in line with the accompanying policy on school photography.
    - Academic record – subjects studied, class assignments, examination results as recorded on official School reports
    - Records of significant achievements
    - Whether the student is exempt from studying Irish
    - Records of disciplinary issues/investigations and/or sanctions imposed

- 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 and Children First Act 2015).

(b) 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 "School Photography Policy"
- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirement for attendance at Primary School.
- 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 other educational settings.

(c) Location and Security:

1. Manual records are kept in a secure, locked filing cabinet in a locked administration office 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.
2. Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office. School has burglar alarm set in closed hours.

C. *Board of Management records:*

(a) Categories of Board of Management data:

- 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 individuals.

(b) 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.

(c) Location and Security:

1. Manual records are kept in a secure, locked filing cabinet in a locked administration office 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.
2. Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office. School has burglar alarm set in closed hours.

D. *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:

Creditors

(a) 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.

(b) 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.

(c) Location and Security:

1. Manual records are kept in a secure, locked filing cabinet in a locked administration office 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.
2. Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office. School has burglar alarm set in closed hours.

Assessment Records

(a) Categories

- Individual Class Teachers will maintain an assessment folder for their current class listing ongoing class assessments, e.g. weekly test results, teacher designed assessment tasks, portfolio material, etc.
- The school will hold data comprising of annual standardised/screening assessment results in respect of its students
- The school may administer diagnostic assessments/screening which provides the school with a more in-depth analysis of a pupil's academic progress.
- An annual school report is issued for each student.
- Individuals' Continuum of Support

(b) Purpose

The rationale for seeking and retaining assessment records is as follows:

- to monitor a student's progress.
- to enable each student to develop to his/her potential
- to meet the educational, social, physical and emotional requirements of the student
- to furnish documentation/information 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 secondary schools (which have confirmed enrolment of the pupils concerned) with 'Education Passports'

(c) Location

- Teacher's Lockable Desk
- Principal's Office
- Copies of Annual Pupil Reports
- Aladdin Schools Online Management Information System
- Designated password protected school server

(d) Security

- Each class teacher and any visiting Department of Education and Skills Inspector requires access to the class based assessment folder. These files are daily, working documents. They will be stored in the teacher's lockable desk and the school server
- There is a secure, locked filing cabinet designated for individual Past pupil files containing annual pupil reports in the Principal's Office
- The Aladdin Schools Online Management Information System stores standardised assessment, screening results and Continuums of Support. It is password protected and a service user agreement is in place
- The Principal, Deputy Principal, School Secretary and Class Teacher have authorised access to these files.
- Employees are required to maintain the confidentiality of any data to which they have access.

Volunteers/Students

(a) Categories

Volunteers, Student Teachers, Student SNAs and Transition Year Students for work experience with personal details e.g. name, address, PPSN, references, insurance details, supervisor contact details

(b) Purposes

Work Experience and volunteering within this school

(c) Location

Manual files are kept for Students for the current school year only. Manual files for volunteers are kept for the duration of the period spent volunteering in the school and for one year after completion.

Data is kept 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.

(d) Security

These records are kept as manual records (personal file within a relevant filing system) and may also be kept as a computer record (database) on the school server/cloud that is password protected. All sensitive personal information will be kept on the Principal's computer only.

Charity tax-back forms

(a) Categories of data: the school may hold the following data in relation to donors who have made charitable donations to the school:

a) name
b) address
c) contact details
d) PPS number
e) tax rate
f) signature
g) gross amount of the donation

(b) 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 parent's 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.

(c) Location and Security:

1. Manual records are kept in a secure, locked filing cabinet in a locked administration office 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.
2. Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office. School has burglar alarm set in closed hours.
3. **CCTV images/recordings** Recorded data is stored on the recording device and is over written after a certain period of time (approximately 30 days). All recorded CCTV data is kept in the Enable Ireland office next to reception, which is locked and secure. 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. To access the CCTV data a written request must be made to Enable Ireland.

   CCTV is installed in Enable Ireland Sandymount School
   - Cameras are installed externally (around the school perimeter)
   - Cameras are installed internally in the common areas (main reception, corridors and GP area

   These CCTV systems may record images of staff, pupils and members of the public who visit the premises.

Examination results

(a) Categories: The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual and continuous assessment results related to the Junior Cert level 1 and 2.

(b) 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 guardian about educational attainment levels and recommendations for the future. 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.

(c) Location and Security

1. Manual records are kept in a secure, locked filing cabinet in a locked administration office 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.
2. Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office. School has burglar alarm set in closed hours.

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:

- POD: [Pupil Online Database]: Collection of the data for the purposes of complying with the Department of Education and Skills pupil online database.
- Child Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Enrolment Policy
- ICT Acceptable Usage Policy
- Assessment Policy
- Critical Incident Policy
- Student Council Policy
- Attendance Policy

Processing in line with 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) Prevent the processing of their data for direct-marketing purposes
c) Ask to have inaccurate data amended
d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.
e) Know what personal data the school is keeping on them

Dealing with a 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)
- The identity of the requestor must be established before the disclosure of any information, and in the case of information requested about a child, checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

  - Passport

- Driving licence
- Utility bills with current address
- Birth/marriage certificate
- Public Services Identity Card

(This list is not exhaustive)

- Request must be responded to within 40 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. Ask for the phone number and contact the caller back once number has been checked.
- 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.

Data security and safeguarding of personal information

Enable Ireland Sandymount School recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

In order to assure the protection of all data being processed and inform decisions on processing activities, the school has undertaken an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in relation to holding their personal data; Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of external Data Processors shall also be considered and these organisations shall be requested to provide evidence of their competence in the security of shared data.

Paper documents

All paper documents containing person-identifiable information is to be stored in a locked cabinet or drawer with access restricted to staff members who need to process that data.

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

Paper documents containing person identifiable information are not permitted to be taken from Enable Ireland Sandymount School to work on at home other than in VERY EXCEPTIONAL CIRCUMSTANCES (e.g. a prolonged pandemic lockdown, extreme weather conditions). In these circumstances, staff will receive training on how to keep those paper documents safe, with reference to advice of the Data Protection Commission relating to home-working and data security.

Electronic data

Electronic data will be selected for removal at the appropriate time and deleted following approval from the Data Controller.

Disposal of electronic hardware

The Data Controller must be informed for authorisation prior to the disposal of all computer equipment.

If a piece of computer equipment is to be disposed of, all personal data on the hard drive is removed before disposal. It will not be sufficient to only 'delete' the unwanted files; they must be permanently removed by overwriting it or removing the hard drive and physically destroying it.

Electronic system security

All computers used by the school are password protected and the system administrator regularly have all passwords changed. No password is to be displayed on a computer or monitor.

The school has laptops that are meant to be used by staff at home in case of remote learning or pandemic. These laptops are encrypted and use Enable Ireland's Infrastructure (such as anti-virus and firewall) to connect to the school server space.

All staff has been given password protected usb memory sticks to store relevant documents. These memory sticks will self-delete all data in it after 3 wrong login attempts.

A user leaving their laptop or desktop should ensure that they lock their computer (by holding Ctrl + Alt + Del and then choosing 'lock this computer') for the duration they are absent from their desk. All computers should be set to sleep after a few minutes of being left idle.

Access to shared folders on the server is managed by the system administrator (Enable Ireland IT Department) who will organise that permissions at the correct level and passwords are controlled and managed appropriately. When staff leave the school's employment the system administrator will ensure that all permissions and password access to all school systems is revoked.

Personal Data Breaches

All incidents in which personal data has been put at risk must be reported to the Office of the Data Protection Commissioner within 72 hours.
When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the BOM must communicate the personal data breach to the data subject without undue delay.
If a data processor becomes aware of a personal data breach, it must bring this to the attention of the data controller (BOM) without undue delay.
See the Enable Ireland Sandymount School Breach Code of Practice (Appendix 4) for more information.

Complaints

Complaints in relation to the procedures contained in this policy should be made to the Chairperson of the Board of Management in writing and sent to the school address. The Chairperson as Data Controller will then decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaints procedure.

Complaints which are not appropriate to be dealt with through the Enable Ireland Sandymount School Complaint's procedure can be dealt with by the Data Protection Commissioner. Contacts details of both are provided with the disclosure information.

Implementation arrangements, 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/ DOP
Teaching personnel:	Awareness of responsibilities
Secretary:	Security, confidentiality

Ratification and Communication

A copy of Enable Ireland Sandymount School's Data Protection Policy is available from the Principal on request. The Data Protection Policy was ratified by the Board of Management of Enable Ireland Sandymount School following consultation with parents and school staff. It is now the school's

agreed Data Protection Policy. All relevant personnel will be made aware of their responsibilities under the policy by the Data Controller.

It is important that all concerned are made aware of any changes implied in recording information on pupils, staff and others in the school community.

Parents/guardians and students should be informed of the Data Protection Policy from the time of expression of interest in a school place for their child. This Data Protection Policy will be included as part of the Admission Pack and on request from the School Office.

Reviewing and evaluating the policy

The policy will be reviewed and evaluated after two years. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or Tusla, the Child and Family Agency), legislation and feedback from parents/guardians, students, school staff and others. The policy will be revised as necessary in the light of such review and evaluation and within the framework of school planning.

Signed:

For and behalf of Board of Management

Date ratified:

Appendix 1 Data Access request form

Enable Ireland Sandymount School

Data Protection Subject Access request (SAR) Application form

Request for access to Personal Data under the General Data protection Regulation (GDPR) and Data Protection Acts 1988-2018

Date issued to data subject:	School Stamp:

Please Note:
In order to respond to your request for personal data, you will need to provide us with adequate Proof of Identity:

- Passport
- Driving licence
- Utility bills with current address
- Birth/marriage certificate
- Public Services Identity Card

(This list is not exhaustive)

Data Retention

We will only keep a copy of these documents until your subject access request has been fully processed and issued to you and all relevant review or appeal proce dure timelines have expired.

Please complete all parts of this Form in full

Full Name	
Maiden Name (if name used during your school duration)	
Address	
Contact Number*	Email Address*

* We may need to contact you to discuss your access request

Please tick the box which applies to you:

Current Pupil	Parent/Guardian	Past Pupil	Current Staff	Past Staff

Details of Data Subject

Please provide the following information:

Name of Subject:		
Date of Birth:		
Insert year of leaving:		
Insert years of start and end:	**From:**	**To:**

Declaration:

Section 3 Data Access Request:

I, ...[insert name] wish to be informed whether or not Enable Ireland Sandymount School, DES Roll No. 18370J, holds personal data about me/my child and to be provided with a description of this data and to be informed of the purpose for holding such data. I am making this access request under Section 3 of the Data Protection Acts.

OR

Section 4 Data Access Request:

I, ... [insert name] wish to make an access request for a copy of any personal data that Enable Ireland Sandymount School,, DES Roll No. 18370J, holds about me/my child. I am making this access request under Section 4 of the Data Protection Acts.

Section 4 Data Access Request only:

Any other information relevant to your access request please state the date, time and location of the images/recordings (otherwise it may be very difficult or impossible for the school to locate the data).

Signature: _____ Date _____

Print Name: _____

Checklist – Have you completed to the following?

1) Completed the Access Request Form in full?
2) Signed and dated the Access Request Form?
3) Included a photocopy of official/State photographic identity document (driver's licence, passport etc.) *

***Note to school**: the school should satisfy itself as to the identity of the individual and make a note in the school records that identity has been provided, but the school should not retain a copy of the identity document.

Please return this form to:

The Chairperson of the Board of Management, Enable Ireland Sandymount School, Sandymount Avenue, Dublin 4, D04 XH22

Appendix 2 - SCHOOL PRIVACY NOTICE TO PUPILS AND THEIR PARENTS AND GUARDIANS

Enable Ireland Sandymount School

SCHOOL PRIVACY NOTICE TO PUPILS AND THEIR PARENTS/GUARDIANS

By enrolling in and attending **Enable Ireland Sandymount School** you and your child acknowledge that you and your child's personal data (including your child's special category personal data) shall be processed by the School.

This Privacy Notice gives you some helpful information about who we are, what personal data we collect about you, why, who we share it with and why, how long we keep it, and your rights.

If you need more information, please request a copy of our Data Protection Policy & Procedures, which is available from the School Office.

1. Who we are:

We are Enable Ireland Sandymount School.

Our address and contact details are:

Enable Ireland Sandymount School,

Sandymount Avenue, Dublin 4,

D04 XH22

Tel: 01 261 5907

Email: sandymountschool.office@enableireland.ie

We provide primary education to children who are aged between 3 and 12 years with a clinical diagnosis of autism and mild or above level of intellectual function and other associated difficulties.

2. The information we collect about you

When you are a pupil with Enable Ireland Sandymount School, we collect and use your personal data.

The personal data we collect can include information about your identity and contact details; images/photo; family details; admission/enrolment details; previous schools; academic progress; PPS number; special educational needs; nationality; language; religion; medical data; information about behaviour and attendance; information about health, safety and welfare; financial information (re fees, grants, etc); and other personal data.

Further details of the data we collect about you can be found in the section on Data in the Data Protection Policy which is available on request from the School Office.

If you are under 18 years when you enrol, we collect the name, address, contact details and other information about your parents/guardians. If you are under 18 years, your parent/guardian is consulted and asked to give consent for certain things like taking your photograph, going on school trips etc.

3. How we use your information and the legal basis

We use your personal data for purposes including:

- your application for enrolment;
- to provide you with appropriate education and support;
- to monitor your academic progress;
- to care for your health and well-being;
- to care for our staff and students; • to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an education body;
- to comply with our monitoring and reporting obligations to Government bodies,
- to process appeals, resolve disputes, and defend litigation etc.

For further information on what data we collect, why we collect it, how we use it, and the legal basis for same, please go to the section on Data in the Data Protection Policy which is available on request from the School Office.

4. Who we share your information with

We share your personal data with third parties, including other Government bodies.

This includes the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, An Garda Síochána, HSE, the Department of Social Protection, the Revenue Commissioners etc.

The level of sharing and the nature of what is shared depend on various factors. The Government bodies to which we transfer your personal data will use your personal data for their own purposes (including: to verify other information they already hold about you, etc) and they may aggregate it with other information they already hold about you and your family. We also share your personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc), We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations. For further information on who we share your data with, when and in what circumstances, and why, please see the section on Data Sharing in our Data Protection Policy which is available on request from the School Office.

5. We do not transfer your personal data to a third country or international organisation.

6. We do not engage in automated decision making/profiling.

7. How long we hold your data

Some personal data is only kept for a short period (e.g. We will destroy at the end of an academic year because it is no longer needed). Some data we retain for a longer period (e.g. retained after you leave or otherwise finish your studies with Enable Ireland Sandymount School). For further information on the retention periods, please go to Appendix 3 of our Data Protection Policy which is available on request from the School Office.

8. You have the following statutory rights that can be exercised at any time:

(a) Right to complain to supervisory authority.
(b) Right of access.
(c) Right to rectification.
(d) Right to be forgotten.
(e) Right to restrict processing.
(f) Right to data portability.
(g) Right to object and automated decision making/profiling.

For further information, please see our Data Protection Policy which is available on request from the School Office.

9. Contact

We are waiting to be advised by the Department of Education and Skills with regard to the appointment of a Data Protection Officer (DPO). Enable Ireland Sandymount School will notify you immediately following notification of the name and contact details of this person.

or

If you would like to discuss anything in this privacy notice, please contact the School Principal by email to sandymountschool.principal@enableireland.ie

Appendix 3: School Retention Record Schedule

SCHOOL RETENTION RECORD SCHEDULE

Schools, as *data controllers* must be clear about the length of time for which personal data will be kept and the reasons why the information is being retained. In determining appropriate retention periods, regard must be had for any statutory obligations imposed on a data controller. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner. It may also be anonymised to remove any personal data. Anonymisation must be irrevocable; removing names and addresses may not necessarily be sufficient.

In order to comply with this legal requirement, *Enable Ireland Sandymount School* has assigned specific responsibility and introduced procedures for ensuring that files are purged regularly and securely and that personal data is not retained any longer than is necessary. All records will be periodically reviewed in light of experience and any legal or other relevant indications.

The following comprises the School Retention Record Schedule for personal data held by Enable Ireland Sandymount School:

Student Records	Final disposition	Comments
Registers/Roll books	Never destroy	Archive when class leaves + 2 years
State exam results	N/A	SEC responsibility to retain, not a requirement for school/ETB to retain.

Records relating to pupils/students	Final disposition	Comments
Enrolment Forms	Never destroy	Archive when class leaves + 2 years
Student transfer forms (Applies from one school to another)	Never destroy	Archive when class leaves + 2 years
Disciplinary notes	Never destroy	Archive when class leaves + 2 years
Results of in-school tests/assessments (i.e. ongoing, end of term, end of year.	Never destroy	Archive when class leaves + 2 years
End of term/year reports	Never destroy	Archive when class leaves + 2 years

Records of school tours/trips, including permission slips, itinerary reports	Never destroy	Archive when class leaves + 2 years

Sensitive Personal Data Students	Final disposition	Comments
Professional reports	Never destroy	Archive when class leaves + 2 years
Special Education Needs' files, reviews, correspondence and Personal Pupil Plans/Individual Education Plans/Care Plans	Never destroy	Archive when class leaves + 2 years
Accident reports	Never destroy	Archive when class leaves + 2 years
Child protection records	Never destroy	Archive when class leaves + 2 years
Section 29 appeal records	Never destroy	Archive when class leaves + 2 years
Enrolment/transfer forms where child is not enrolled or refused enrolment	Never destroy	Archive when class leaves + 2 years
Records of complaints made by parents/ guardians	Confidential shredding or never destroy, depending on the nature of the records/ complaint.	Depends entirely on the nature of the complaint. If it is child-safeguarding, a complaint relating to teacher-handling, or an accident, then retain indefinitely. Never destroy. If it is a complaint of a more mundane nature (e.g. misspelling of child's name, parent not being contacted to be informed of parent-teacher meeting) or other minor matter, then student reaching 18 years + 7 years (6 years in which to take a claim, and 1 year for proceedings to be served on school)

Staff Records	Final disposition	Comments
Applications & CVs of candidates called for interview	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Database of applications	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Selection criteria	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Applications of candidates not shortlisted	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Unsolicited applications for jobs	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Candidates shortlisted but unsuccessful at interview	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Candidates shortlisted and are successful but do not accept offer	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Interview board marking scheme & board notes	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Panel recommendation by interview board	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.

Staff personnel files (whilst in employment)	Final Disposition	Comments
e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, records of staff training etc.	Confidential shredding. Retain an anonymised sample for archival purposes.	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Application &/CV	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Qualifications	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
References	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview: database of applications (the section which relates to the employee only)	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Selection criteria	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview board marking scheme & board notes	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Panel recommendation by interview board	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Recruitment medical	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)

Job specification/ description	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Contract/Conditions of employment	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Probation letters/forms	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
POR applications and correspondence (whether successful or not)	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Leave of absence applications	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Job share	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Career Break	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Maternity leave	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Paternity leave	Confidential shredding	Retain for 2 years following retirement/resignation or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).
Parental leave	Confidential shredding	Must be kept for 8 years - Parental Leave Act 1998. Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years.
Force Majeure leave	Confidential shredding	Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)

		(whichever is the greater). There is a statutory requirement to retain for 8 years.
Carers leave	Confidential shredding	Must be kept for 8 years - Carer's Leave Act 2001 Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years
Working Time Act (attendance hours, holidays, breaks)	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school). There is a statutory requirement to retain for 3 years
Allegations/complaints		Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). **Please note** the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.
Grievance and Disciplinary records		Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). **Please note** the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.

Occupational Health Records	Final Disposition	Comments
Sickness absence records/certificates	Confidential shredding Or do not destroy.	Re sick leave scheme (1 in 4 rule) ref DES C/L 0060/2010 Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Pre-employment medical assessment	Confidential shredding Or do not destroy?	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Occupational health referral	Confidential shredding Or Do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Correspondence re retirement on ill-health grounds	Confidential shredding Or Do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Accident/injury at work reports	Confidential shredding	Retain for 10 years, or the duration of the employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), whichever is the greater (unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy).
Medical assessments or referrals	Confidential shredding Or Do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless Medmark assessment relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Sick leave records (sick benefit forms)	Confidential shredding	In case of audit/refunds, Current year plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)

Superannuation /Pension /Retirement records	Final Disposition	Comments
Records of previous service (incl. correspondence with previous employers)		DES advise that these should be kept indefinitely.
Pension calculation	Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)
Pension increases (notification to Co.)	Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)
Salary claim forms	Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)

Government returns	Final disposition	Comments
Any returns which identify individual staff/pupils,		Depends upon the nature of the return. If it relates to pay/pension/benefits of staff, keep indefinitely as per DES guidelines. If it relates to information on students, e.g. October Returns, Annual Census etc., keep in line with "Student Records" guidelines above.

Board of Management Records	Final disposition	Comments
Board agenda and minutes	Do not destroy	Indefinitely. These should be stored securely on school property
School closure	Do not destroy	On school closure, records should be transferred as per Records Retention in the event of school closure/amalgamation. A decommissioning exercise should take place with respect to archiving and recording data.

Other school based reports/minutes	Final disposition	Comments
Principal's monthly report including staff absences	Do not destroy	Indefinitely. Administrative log and does not relate to any one employee in particular: the monthly reports are not structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Not a "relevant filing system".

Financial Records	Final disposition	Comments
Audited Accounts	Do not destroy	Indefinitely
Payroll and taxation	Do not destroy	Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained **indefinitely** within the school. These records can be kept either on a manual or computer system.

Invoices/back-up records/receipts		Retain for 7 years

Promotion process	**Final Disposition**	**Comments**
Posts of Responsibility	Do not destroy	Retain indefinitely on master file as it relates to pay/pension etc. (See DES guidelines)
Calculation of service	Do not destroy	Retain indefinitely on master file
Promotions/POR Board master files	Do not destroy	Retain indefinitely on master file
Promotions/POR Boards assessment report files		Retain original on personnel file in line with retention periods in "Staff Records" retention guidelines above
POR appeal documents		Retain original on personnel file, and copy of master & appeal file. Retain for duration of employment + 7 years (6 years in which to take a claim, plus 1 year to serve proceedings on school). Copy on master and appeal file.
Correspondence from candidates re feedback		Depends upon nature of feedback. If feedback is from unsuccessful candidate who is not an employee within the school, keep in line with retention periods in "Staff Records" above. If feedback is from successful candidate or from unsuccessful candidate who is already an employee within the school, keep in line with "Staff personnel while in employment" above.

Principal / Deputy Principal appointment	Final Disposition	Comments
Successful Applicants		All records relating to the successful applicant should be retained by the school for the duration of employment+7 years. Records include: • A copy of the advertisement. • The Principal's/Deputy Principal's application for the post. • Criteria for assessment of applicants. • Any documents and/or notes created by the Interview Board. • The Interview Board Report – including confirmation of verification of references from previous employers. • A copy of the Principal's/Deputy Principal's educational qualifications e.g. initial teacher education qualifications, Post Graduate courses or Masters Degrees. • A copy of the Registration Certificate for the Principal/Deputy Principal Teacher from the Teaching Council of Ireland. • Confirmation of compliance with the National Vetting Bureau (Children and Vulnerable Persons) Acts 2012 to 2016 and with relevant Department Circulars in relation to Garda vetting. • A copy of the confirmation of medical fitness received from the Occupational Health Service. • Any other relevant documentation relating to individual Principal/Deputy Principal appointment. • Record of the Patron's/CE's approval of the appointment. • One part completed contract of employment i.e. signed by the employer and the Principal/Deputy Principal. • A copy of the appointment form completed by both parties that was submitted to the Paymaster.
Unsuccessful Applicants		All records relating to the successful applicant should be retained by the school for the duration of employment+7 years. Records include: • A copy of the advertisement. • The Principal's/Deputy Principal's application for the post.

		• Criteria for assessment of applicants. • Any documents and/or notes created by the Interview Board. • The Interview Board Report – including confirmation of verification of references from previous employers. • A copy of the Principal's/Deputy Principal's educational qualifications e.g. initial teacher education qualifications, Post Graduate courses or Masters Degrees. • A copy of the Registration Certificate for the Principal/Deputy Principal Teacher from the Teaching Council of Ireland. • Confirmation of compliance with the National Vetting Bureau (Children and Vulnerable Persons) Acts 2012 to 2016 and with relevant Department Circulars in relation to Garda vetting. • A copy of the confirmation of medical fitness received from the Occupational Health Service. • Any other relevant documentation relating to individual Principal/Deputy Principal appointment. • Record of the Patron's/CE's approval of the appointment.

Appendix 4 **Enable Ireland Sandymount School Personal Security Breach Code of Practice**

Enable Ireland Sandymount School Personal Security Breach Code of Practice

Purpose of Code of Practice

This Code of Practice applies to Enable Ireland Sandymount School as data controller [ ]. This Code of Practice will be:

1. available on the school website
2. circulated to all appropriate data processors and incorporated as part of the service-level agreement/data processing agreement between the school and the contracted company and
3. shall be advised to staff at induction and at periodic staff meeting(s) or training organised by the school.

Obligations under Data Protection

The school as data controller and appropriate data processors so contracted are subject to the provisions of the Data Protection Acts 1988 to 2018 and the European Union General Data Protection Regulation 2018 and exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

The school has prepared a Data Protection Policy and monitors the implementation of this policy at regular intervals. The school retains records (both electronic and manual) concerning personal data in line with its Data Protection Policy and seeks to prioritise the safety of personal data and particularly sensitive personal data, so that any risk of unauthorized disclosure, loss or alteration of personal data is avoided.

Protocol for action in the event of breach

In circumstances where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the school will follow the following protocol:

1. The school will seek to contain the matter and mitigate any further exposure of the personal data held. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and requesting that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.
2. Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011. The penalties for withholding information include a fine of up to €5,000 or 12 months' imprisonment on summary conviction.

3. Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the school may conclude that there is no risk to the data and therefore no need to inform data subjects or contact the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

4. Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (2) above.

5. Contact should be immediately made with the data processor responsible for IT support in the school.

6. In addition and where appropriate, contact may be made with other bodies such as the HSE, financial institutions etc.

7. Reporting of incidents to the Office of Data Protection Commissioner: All incidents in which personal data (and sensitive personal data) have been put at risk shall be reported to the Office of the Data Protection Commissioner as soon as the school becomes aware of the incident (or within 72 hours thereafter), save in the following circumstances:

• When the full extent and consequences of the incident have been reported without delay directly to the affected data subject(s) and
• The suspected breach affects no more than 100 data subjects and
• It does not include sensitive personal data or personal data of a financial nature [ ].

Where all three criteria are not satisfied, the school shall report the incident to the Office of the Data Protection Commissioner within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident (see further details below). Where no notification is made to the Office of the Data Protection Commissioner, the school shall keep a summary record of the incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record shall comprise a brief description of the nature of the incident and an explanation why the school did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records shall be provided to the Office of the Data Protection Commissioner upon request.

8. The school shall gather a small team of persons together to assess the potential exposure/loss. This team will assist the principal of the school with the practical matters associated with this protocol.

9. The team will, under the direction of the principal, give immediate consideration to informing those affected [ ]. At the direction of the principal the team shall:
• Contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.
• Where possible and as soon as is feasible, the data subjects (i.e. individuals whom the data is about) should be advised of:

- the nature of the data that has been potentially exposed/compromised;
- the level of sensitivity of this data and an outline of the steps the school intends to take by way of containment or remediation.

• Individuals should be advised as to whether the school intends to contact other organisations and/or the Office of the Data Protection Commissioner.
• Where individuals express a particular concern with respect to the threat to their personal data, this should be advised back to the principal who may, advise the relevant authority e.g. Gardaí, HSE etc.
• Where the data breach has caused the data to be "damaged" (e.g. as a result of hacking), the

principal shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.
• The principal shall notify the insurance company which the school is insured and advise them that there has been a personal data security breach.

10. Contracted companies operating as data processors: Where an organisation contracted and operating as a data processor on behalf of the school becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the school as a matter of urgent priority. In such circumstances, the principal of the school should be contacted directly. This requirement should be clearly set out in the data processing agreement/contract in the appropriate data protection section in the agreement.

11. A full review should be undertaken using the template Compliance Checklist and having regard to information ascertained deriving from the experience of the data protection breach. Staff should be apprised of any changes to the Personal Data Security Breach Code of Practice and of upgraded security measures. Staff should receive refresher training where necessary.

Further advice: What may happen arising from a report to the Office of Data Protection Commissioner?

• Where any doubt may arise as to the adequacy of technological risk-mitigation measures (including encryption), the school shall report the incident to the Office of the Data Protection Commissioner within 72 hours of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be by e-mail, telephone or fax and shall not involve the communication of personal data.
• The Office of the Data Protection Commissioner will advise the school of whether there is a need for the school to compile a detailed report and/or for the Office of the Data Protection Commissioner to carry out a subsequent investigation, based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.
• Should the Office of the Data Protection Commissioner request the school to provide a detailed written report into the incident, the Office of the Data Protection Commissioner will specify a timeframe for the delivery of the report into the incident and the information required. Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised
- the action being taken to secure and/or recover the personal data that has been compromised
- the action being taken to inform those affected by the incident or reasons for the decision not to do so
- the action being taken to limit damage or distress to those affected by the incident
- a chronology of the events leading up to the loss of control of the personal data; and
- the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the school has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.