GDPR POLICY

1. GDPR Compliance Statement

The characteristic spirit of Enable Ireland Sandymount School has at its core a desire to promote and protect the dignity of every member of its community, students, staff and parents. This includes respect for the protection of data stored at the school and for the right of access to this data. This policy is informed by these aspirations and also the General Data Protection Regulation (GDPR) which came into force across the European Union on 25th May 2018. The policy applies to all school staff, the Board of Management, parents/guardians, students, (including prospective students) their parents/guardians, applicants for positions within the school and service providers with access to school data.

Enable Ireland Sandymount School is aware of its responsibilities as a controller of personal data under GDPR. The school has been briefed as to its scope and implications for our school. All members of staff at Enable Ireland Sandymount School who will be involved in processing personal information will be informed appropriately as to their responsibilities with respect to GDPR in their day to day work.

As a school, we have always been committed to high standards of data protection, information security & privacy.

Enable Ireland Sandymount School respects the privacy of students, staff and visitors to the school and is committed to protecting their personal data.

We will safeguard the personal information under our remit and develop a robust data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation of the GDPR.

Our GDPR Principles:

- We will process all personal data fairly and lawfully;
- We will only process personal data for specified and lawful purposes;
- We will endeavour to hold relevant and accurate personal data, and where practical, we will keep this up to date;
- We will not retain personal data for longer than is necessary;
- We will keep all personal data secure;
- We will endeavour to ensure that personal data is not transferred to countries outside of the European Economic Area ('EEA') without adequate protection.

The detailed arrangements for achieving these objectives are set out in the main body of this policy. The Principal together with the Board of Management has overall responsibility for data protection at the school.

This policy requires the co-operation of all staff, visitors, contractors and others to enable our school to discharge its responsibilities under the GDPR.

Enable Ireland Sandymount School is committed to upholding the standards outlined in this policy. Sufficient authority and resources, both financial and otherwise, will be made available to enable the school to carry out their responsibilities under the GDPR. All employees will be made aware of and have access to this policy.

2. Purpose and Scope

- The purpose of this Data Protection Policy is to support the school in meeting its responsibilities with regard to the processing of personal data. These responsibilities arise as statutory obligations under the relevant data protection legislation. They also stem from our desire to process all personal data in an ethical manner which respects and protects the fundamental rights and freedoms of natural persons.
- This policy aims to help transparency by identifying how the school expects personal data to be treated (or "processed"). It helps to clarify what data is collected, why it is collected, for how long it will be stored and with whom it will be shared.
- The Irish Data Protection Act (2018) and the European General Data Protection Regulation (2016) are the primary legislative sources.1 As such they impose statutory responsibilities on the school as well as providing a number of fundamental rights (for students, parents/guardians and staff and others) in relation to personal data.
- The school recognises the seriousness of its data processing obligations and has implemented a set of practices to safeguard personal data. Relevant policies and procedures apply to all school staff, boards of management, trustees, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school).
- Any amendments to this Data Protection Policy will be communicated through the school website and other appropriate channels, including direct communication with data subjects where this is appropriate. We will endeavour to notify you if at any time we propose to use Personal Data in a manner that is significantly different to that stated in our Policy, or, was otherwise communicated to you at the time that it was collected.
- 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. Formally, the statutory responsibility of Controller is assigned to the Board of Management. The Principal is assigned the role of co-ordinating the implementation of this Policy and for ensuring that all staff who handle or have access to Personal Data are familiar with their responsibilities.

Name	***Responsibility***
Board of Management	Data Controller
Principal	Implementation of Policy
All Staff	Adherence to the Data Processing Principles
Entire School Community	Awareness and Respect for all Personal Data

3. Legal Obligations

In the addition to our obligations under GDPR, the implementation of this policy takes into account the school's other legal obligations and responsibilities in the Public Interest. Some of which are directly relevant to data protection:

- Under Section 9(g) of the Education Act, 1998, ensure that parents of a student, or in the case of a student who has reached the age of 18 years, the student, have access in the prescribed manner to records kept by that school relating to the progress of that student in his or her education;
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School;

- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring;
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day;
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply Personal Data kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training);
- Under Section 14 of the Education for Persons with Special Educational Needs 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 2014 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 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).

4. GDPR Principles

4.1 Lawfulness, fairness and transparency

Enable Ireland Sandymount School believes in operating our school fairly and ethically and this will extend to all personal data held for those purposes. Subjects will be informed when data is being collected, and at the same time informed what we will use that data for. We will ensure that appropriate technical and organisational measures are in place to secure that data.

Collection and processing of data will be transparent. Advisory notices and privacy notices relating to data rights will be published as appropriate in plain English and will be structured where relevant to improve accessibility of this information to data subjects. Persons will be clearly advised of their rights also.

4.2 Purpose Limitation

Personal data collected by Enable Ireland Sandymount School will be processed only for the purpose for which it was collected. In the event that this purpose should change, data subjects will be informed within the 30-day regulatory period and consent sought for the change.

4.3 Data Minimisation

Enable Ireland Sandymount School will collect only the minimum quantity of personal data to carry out a particular task. Where appropriate, potential data subjects will be requested not to provide unwanted or inappropriately sensitive personal information.

4.4 Data Accuracy

Enable Ireland Sandymount School will make every effort to ensure that subjects' information is accurate and up to date. Enable Ireland Sandymount School will endeavour to ensure via appropriate levels of staff training that it is transcribed accurately. If it is not possible for subjects to correct their data personally, data can be corrected by contacting Reception.

4.5 Storage Limitation

Enable Ireland Sandymount School will store and retain personal data only while there is a valid and lawful basis to do so. Personal information will be deleted when it is no longer required for the purposes for which it was collected.

Where systems do not allow deletion of all records relating to an individual, records will be anonymised by replacing personal information fields with substituted generic text.

4.6 Integrity & Confidentiality

Personal Data shall be processed securely i.e. in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage. Enable Ireland Sandymount School will use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

4.7 Accountability

Enable Ireland Sandymount School is responsible for, and is able to demonstrate compliance with GDPR. This means Enable Ireland Sandymount School will demonstrate that these Data Protection Principles (as outlined here) are met for all Personal Data for which it is responsible.

5. Data Subjects Rights

5.1 Rights of Data Subjects

Enable Ireland Sandymount School recognises the following as the rights of Data Subjects in certain circumstances:

- The right to make Subject Access Requests (SARs);
- The right to have inaccuracies corrected (rectification);
- The right to have information erased (right of erasure);
- The right to restrict the processing of information (restriction);
- The right to be informed on why personal data is processed (notification);
- The right to Data Portability;
- The right to object to processing of personal data (object);
- The right not to be subject to decisions based on automated decision making.

5.2 Right of Access (Also known as a Subject Access Request) (Article 15 of GDPR)

Data Subjects have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data;

- Other supplementary information;

Right of access requests must be responded to within one month through the Principal.

5.3 Right to Rectification (Article 16 of GDPR)

Data Subjects are entitled to have their personal data rectified if it is inaccurate or incomplete. If the information in question has been disclosed to a third party the Data Controller must inform them of the request for rectification where possible. The Data Subject is also entitled to be informed of the third parties to whom the data has been disclosed, where appropriate.

Rights to rectification must be responded to within one month.

5.4 Right to Erasure (Article 17 of GDPR)

This Right is also known as the 'Right to be Forgotten'. It enables Data Subjects to request the deletion or removal of personal data where there is no compelling reason for its continued processing by the Data Controller.

The Right to Erasure applies in the following circumstances:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected;
- The processing was based on consent, and the Data Subject has now withdrawn their consent;
- The Data Subject objects to processing and there is no overriding legitimate interest of the Data Controller;
- The data was being unlawfully processed;
- The data must be erased to comply with a legal obligation;

On receipt of this request, we will carry out an assessment of whether the data can be erased without affecting the ability of the School / Department of Education to provide future services to you or to meet it statutory obligations for example under the National Archives Act, 1986.

5.5 Right to Restrict Processing (Article 18 of GDPR)

The Right to Restrict Processing applies in the following circumstances:

- When a Data Subject contests the accuracy of their personal data, then processing should be restricted to storage only until accuracy is verified;
- When a Data Subject objects to processing which is being carried out for the reason of performance of a task in the public interest, then the Data Controller must restrict processing to storage only whilst they consider whether their lawful basis for processing override the Rights and freedoms of the individual;
- When processing is unlawful and a Data Subject opposes the use and requests restriction to storage instead;
- When the Data Controller no longer needs the personal data but the Data Subject requires it for the purpose of, or in the defence of a legal claim.

When this Right is exercised, Enable Ireland Sandymount School will carry out an assessment of whether the data can be restricted without affecting the ability of the School / Department of Education to provide future services to you.

5.6 Right to Data Portability (Article 20 of GDPR)

This Right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one service provider to another in a safe and secure way in a common data format e.g. pdf file.

The Right to Data Portability applies in the following circumstances:

- When the personal data was provided to the controller directly by the Data Subject;
- Where the processing is based on consent or performance of a contract;
- When processing is carried out by automated means.

5.7 Right to Object (Article 21 of GDPR)

Individuals have the Right to object to processing based on:

- Legitimate interest or performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling);
- Processing for the purposes of scientific/historical research and statistics.

5.8 Rights in Relation to Automatic Decision Making and Profiling (Article 22 of GDPR)

This Right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. The Right not to be subject to a decision applies when:

- It is based on automated processing;
- It produces legal/significant effects on the individual not apply if the decision;
- Is necessary for entering into or performance of a contract is authorised by law;
- Is based on explicit consent;
- Does not have a legal/significant effect on the data subject.

At present there is no automated processing within the Department of Education.

6. Responsibilities

6.1 Board of Management

Implement appropriate technical and organisational measures and be able to demonstrate that data processing is performed in accordance with the Regulation; review and update those measures where necessary considering at all times (with regard to the processing of personal data):

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;

In addition:

- Review and approve the Data Protection Policy;
- Supporting the Principal in the implementation of this policy;

- Review the implementation, effectiveness and compliance with policies, procedures and protocols;
- Ensure Data Protection Issues are an Agenda item at BOM meetings;
- Ensuring that personal data discussed at Board of Management Meetings is kept secure at all times;

6.2 Senior Management including Principal & Deputy Principals

- Ensure the policy is communicated throughout the school;
- Ensure the policy is implemented throughout the school;
- Ensure personal data relating to students & staff is collected and processed in accordance with this policy;
- 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.
- Ensure that there are regular updates to data protection awareness, so that data protection is a "living" process aligned to the school's ethos.
- Periodically check data held regarding accuracy.
- Driving privacy and data protection awareness in the school;
- Identifying training needs and arranging for refresher training sessions;
- Escalating appropriate issues to the Board of Management;
- Taking appropriate preventative actions to mitigate the risk of data breaches arising;
- Spearheading the response to any data breach (following the data breach protocol);
- Due diligence of service providers (data processors) prior to any service provider being retained;
- Ensuring adequate assurances of GDPR compliance are obtained.
- Ensuring appropriate written contracts in place with all service providers;
- Ensure that Record-keeping of data protection items is carried out;
- Board of Management (BOM) Meetings:
    - Ensure BOM Minutes and records are kept secure in locked filing cabinets at all times;
    - Ensure that electronic versions of BOM Minutes are kept secure in password protected folders;
    - Ensure minutes that identifies vulnerable persons or particularly sensitive data is anonymized where possible.
    - BOM minutes circulated via email to a designated email registered with the school's domain.
    - Ensure that information is kept secure at all times and that the information is shredded as soon as could be reasonably expected.
- • Periodic reviews of all data protection arrangements are carried out.

6.3 Staff

6.3.1 General

- Read and sign acknowledgement of this policy;
- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures. Request clarification if there is uncertainty;
- Check that any information that they provide in connection with their employment is accurate and up to date;
- Adherence to high standards of ethics and professionalism in all data entries (e.g. when entering notes about a student on any system);

- Ensure personal data is kept safe and secure, and is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Ensure personal data related to students is accurately processed in accordance with this policy;
- Ensure personal data (particularly sensitive personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion (e.g. if taking personal data to a TUSLA case conference to review a child, ensure the data are stored securely on an encrypted laptop);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with access requests.

6.3.2 Handwritten Notes / Paper Records

- Handwritten Notes can be lost or mislaid (whether in a journal or otherwise).
- Staff are urged to use the functionality provided on Aladdin and other school systems for taking records etc.
- Staff are advised that they have 3 options when taking handwritten notes:
  - Note is scanned and saved on the school's server in a secure folder, and the note shredded or,
  - Note is transferred to the students file in a secure filing cabinet in a locked office or
  - If none of the above options are appropriate, then the note is destroyed / shredded as per the retention policy;
- Information required for Parent Teacher Meetings may be printed off the school server for that specific purpose providing that the teacher keeps that information secure at all times and that the information is shredded as soon as could be reasonably expected. Under no circumstances will teachers be permitted to take this information off the school premises.

6.3.3 Electronic Records

- When accessing school apps on their own mobile devices and or personal devices, staff will ensure these devices are pin protected, and passwords to school related apps are never saved / cached in the browser or app.
- Should your mobile device get lost / stolen, staff will immediately notify the Principal who will then ensure that login details are reset.
- Ensure that personal data is not visible to others (e.g. never display the S: drive or Aladdin on a projector or leave your computer without logging out or locking the screen);
- School servers / cloud have been provided to ensure availability of data, allowing appropriate back-ups to be made, ensuring accountability, transparency, as well as keeping data safe and secure, etc. Staff are urged to use this infrastructure;
- When working with personal data, all staff must ensure that the screens of their computers / tablets / apps are always locked when left unattended;
- Never storing personal data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Only school supplied software is permitted for the recording of personal data at the school.

6.3.4 Emails

- Prepare emails with high levels of diligence and attention to detail i.e. ensuring that the correct email address is entered; Using "bcc" instead of "to" field where appropriate;
- Limit identifying persons in emails / attachments where at all possible;

- Encrypting emails where appropriate for other uses including the use of "Do Not Forward" etc.;
- Attachments containing personal data should be downloaded, stored securely, and then deleted;
- Data should be encrypted before being transferred electronically where appropriate;
- Staff will not save copies of personal data to their own computers, phones, tablets, USB sticks, Hard Drives;

6.3.5 Records

- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;

6.3.6 Social Media

- Never sharing work-related data on unapproved systems (e.g. talking about a student in a teachers WhatsApp group);

6.3.7 Phishing / Malware

- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Never signing the School up to any apps or software relating to school business, or requiring students to engage with apps/software without the prior written approval of the Principal;
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords;
- Ensure passwords are unique (e.g. do not use the same password for a personal account as for your school account etc);

6.4 Administrators

6.4.1 General

- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures.
- Request clarification if there is uncertainty. Read and sign acknowledgement of this policy;
- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification;
- Keeping Personal Data only as per the Retention Policy to satisfy the permitted uses;
- Ensure data related to students, parents and staff is accurately processed in accordance with this policy;
- Keep the reception area clean and tidy;
- Ensure that personal data is not visible to others (e.g. leaving files on desk);
- Keep personal data out of sight of visitors to reception area;
- Ensure that their computer screen is not visible to visitors at reception;
- Diligence and attention-to-detail when entering data on to the School administrative system;
- Keep the data accurate, complete, and up-to-date;
- Ensuring filing cabinets and office door is kept locked when not in use;

- Prepare post with high levels of diligence and attention to detail. Ensuring that the correct letter is put in the correct envelope. Developing post protocol checklist (e.g. double-checking enclosures, envelope counts, etc);
- Adhere to Enable Ireland's IT security Policy
- Respect access-permission levels, never looking into files/records to which you have no genuine employment reason for accessing, adhering to the principle of "need to know";
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;

6.4.2 Subject Access Request

- Identify data subject requests when they are received (by in person request, letter, email, phone etc). If received by telephone, asking the person to put their request in writing using the "Subject Access Request Form" (appendix 1). Ensuring that all such requests (whether by phone, in person or by email or in writing) are immediately escalated to the Principal without delay;
- Being cautious about requests for information: where a request for personal data is received, asking the requester to verify their identity ascertaining whether the requester is legally entitled to obtain the personal data (Two forms of identification must accompany this form. Acceptable forms of identification include: Copy of current passport or driving licence, copy of bank statement less than 6 months old, copy of utility bill less than 6 months old).

6.4.3 Email

- Prepare emails with high levels of diligence and attention to detail i.e. Ensuring that the correct email address is entered; Using "bcc" instead of "to" field where appropriate; Encrypting emails where appropriate;
- If emailing to a group, verifying who the members of the group are;
- Be cautious and suspicious if an email asks you to click on links or open an attached document (even if from a familiar sender from a genuine email address);

6.4.4 Phishing / Malware

- Ensure that data are kept safe and secure. Use strong passwords (12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for a personal account as for your school account etc);
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering;

6.5 Caretaker / Cleaning Staff

- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures. Request clarification if there is uncertainty;
- Ensure the security of school buildings i.e. locking gates, locking doors;
- Ensure alarms are switched on each evening and working;
- Ensure that only authorised persons have access to School buildings;
- Storage of confidential wastepaper until it is securely shredded;
- Report any personal data breaches immediately to the Principal;

- Comply with and give assistance during audits, spot-checks, and inspections.

6.6 Website / Social Media Coordinator

- Exercise due care when posting photographs on the school's social media channels;
- Ensuring that photos are never shared on social media channels where consent has not been received from the student's parent / guardian, the student's name will never be identified;
- Deleting photographs off their personal device once emailed / posted on the school's social media channels;
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) for all social media / website accounts and change them regularly. Never share log-in credentials i.e. same password for personal social media as school social media accounts.
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;

6.7 Data Processors (Third Parties with whom the school share personal data)

- Process personal data only on documented instructions from the controller, including with regards to transfers of data outside the EEA;
- Ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- A Data Processing Agreement is in place between our school and the third party that strengthens our compliance with the GDPR (appendix 5);
- Take all measures pursuant to Article 32 on security of processing;
- Respect the conditions for enlisting another processor;
- Assist the controller by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests to exercise data subjects' rights;
- Assist the controller in complying with the obligations in Articles 32–36 (security, data protection impact assessments and breach notification), considering the nature of the processing;
- At the choice of the controller, delete or return all personal data to the controller after the end of the provision of data processing services; and
- Make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

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)
- Toptech Fire & Security
- Ark Services

(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 list is not exhaustive

7. Data Protection Policy

7.1 GDPR Awareness

Enable Ireland Sandymount School will ensure that management and staff are aware of GDPR and are trained appropriately to their duties in respect of processing of personal data as per this data protection policy. The training and awareness programme will consist of:

- Briefing to all staff
- Online training sessions trough Ark Services
- A general email to all staff with the Data Protection Policy;

7.2 Balance of Rights

In using personal data for the operation of the school, we will ensure that we will only use a subject's data if the subject's rights do not outweigh our lawful basis in using that data.

The balance will be assessed by first checking that we have a lawful basis for using the data, and then evaluating whether disproportionate financial, reputational or social harm could be caused to the individual through our use of their data. We will achieve this on an ongoing basis via the Data Protection Policy and Record of Processing methods already explained in this policy.

7.3 Data Protection Impact Assessment

Enable Ireland Sandymount School will carry out and record an impact assessment appropriate in scope to the sensitivity of the personal data being processed. This will identify risks to the data subject, to compliance and to the organisation with respect to GDPR principles. This exercise will be repeated as required i.e. when a change in practices causes us to re-evaluate the impact on data privacy.

7.4 Lawful Processing Criteria

Enable Ireland Sandymount School processes personal data in the pursuance of several lawful processing criteria. In all cases we examine the balance of rights with respect to the use of personal data. It is our objective to align our activities with the rights of the data subject, such

that our use of their data is beneficial to the data subject and that any inconvenience or risk to the data subject is minimal in comparison with the benefits there from. We have established our lawful processing criteria in the Data Map & Processing Activities in Section 8.

7.5 Storage and Use of Personal Data

The security of personal data relating to students and staff is a very important consideration under the GDPR and is taken very seriously at Enable Ireland Sandymount School. Appropriate security measures will be taken by the school to protect unauthorised access to this data and to the data it is collecting and storing on behalf of the Department of Education and Skills (DES).

A minimum standard of security will include the following measures:

- Access to the information will be restricted to authorised staff on a "need-to-know" basis;
- Manual files will be stored in a relevant filing system, located away from public areas in locked cabinets;
- Computerised data will be held under password protected files;
- Any information which needs to be disposed of will be done so carefully and thoroughly;
- The premises at Enable Ireland Sandymount School are protected by a private security company and are monitored on a 24 hour/7 day week basis.

7.5.1 Paper based records

Paper based records shall be kept in a secure place where unauthorised people access it. This also applies to data that is usually stored electronically but has been printed out for a valid reason:

- All personnel will ensure that personal data, paper and printouts are not left where unauthorised people could see them;
- When not required, the paper or files will be kept in a relevant filing system in a locked secured filing cabinet or;
- Scanned, transferred to and saved on a password protected folder on the school server / cloud or;
- Data will be shredded and disposed of securely.

7.5.2 Electronic records

When data is stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data will be protected by strong passwords that are changed regularly and never shared between employees;
- Personal Data will only be stored on school supplied equipment / infrastructure i.e. school supplied desktop computers / laptops and school supplied servers, cloud storage;
- Data will be stored on designated drives and servers and will only be uploaded to approved cloud computing services.
- Servers containing personal data will be sited in a secure location.
- Data will be backed up frequently.
- All servers and computers containing data will be protected by approved security software and a firewall.

7.5.3 Use of Student Personal Data

We use student's personal data for purposes including:

- their application for enrolment;

- to provide them with appropriate education and support;
- to monitor their academic progress;
- to care for their 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 the safety of our staff and students and for the protection of personal and school property (use of CCTV).

7.5.4 Use of Staff Personal Data

We use staff personal data for purposes including:

- their application for employment;
- to provide them with appropriate direction and support in your employment;
- to care for their health and well-being;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.;
- for the safety, health & wellbeing of other staff, students and visitors.

Enable Ireland Sandymount School understands that sensitive information may be identified through Garda Vetting. In the event that an employee's Garda vetting raises concerns, the information will be dealt with on a confidential basis. All information pertaining to such a situation will be stored in the same way as other data. The Board of Management will not pass on a copy of a Garda Vetting Form to any other party.

7.6 Sharing Personal Data

From time to time, we may share personal data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, An Garda Síochána, HSE, the Department of Social Protection, our Insurance Company, the Revenue Commissioners etc.

The sharing of student personal data and the nature of what is shared depends on various factors. The Government bodies to which we transfer personal data will use that data for their own purposes (including: to verify other information they already hold etc.) and they may aggregate it with other information they already hold about the data subject and the data subject's 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.

7.7 Special Categories of Data

7.7.1 Children/Students

Special categories of particularly sensitive personal information requires higher levels of protection. The school through the Department of Education may:

- Collect information on ethnic/cultural background of students with the consent of the parent/guardian for statistical analysis and reporting in aggregated format for the purposes of social inclusion and integration.
- Collect data on the religion of the student with the consent of the parent/guardian again for enrolment and statistical purposes.
- Process data related to health in respect of students with special educational needs or a disability for the purpose of ensuring that support services is made available to each child, as defined in section 2 of the Education Act 1998 including psychological services and a level and quality of education appropriate to meeting the needs and abilities of that person.

The Department of Education will only process special categories data relating to children or students for the purposes of allocating resources where this is provided for by way of enactment or the Constitution.

7.7.2 School Staff and Retired School Staff

Special categories of particularly sensitive personal information requires higher levels of protection. The school through the Department of Education may:

- Process data on trade union membership deductions with the consent of the staff member.
- Through the consent of the individual, process religious information where the individual wishes to be addressed by a religious title e.g. Father.
- Process information on sick leave but not the nature of the illness for the purpose of payments to school staff.
- Process data related to health where the occupational health service provides information in respect of applications for retirement on the grounds of ill health.
- Process data related to health when reviewing sample cases as part of an audit of public monies expended in the occupational health service.
- Process information related to religion where a person was or is part of a religious order and the processing of this data is required under the pension schemes.

7.7.3 Photographs of Students

The school maintains a database of photographs from school events held over the years. It has become customary to take photos of students engaged in activities and events in the interest of creating a pictorial as well as historical record of life at the school. Photographs only may be published on our school website, app, on social media or in brochures, yearbooks, newsletters, local and national newspapers and similar school related productions when authorised by parents/guardians.

Consent is requested from each parent when enrolling with the school. Should the parent wish to have his/her child's photograph removed from the school website, electronic brochure, electronic yearbooks, electronic newsletters etc. at any time, we will duly comply on receipt of a written request to the school principal.

Past physical brochures, yearbooks and newsletters will not be possible to withdraw. Parents/ Guardians can request for his/her child's photograph not to be used in future physical publications.

8. Personal Data and related Processing Purposes

Purposes for Processing	Description of Personal Data
1. Contact and identification information This information is needed to identify, contact and enrol students.	
Purposes may include: • to add names to a contact list prior to formal application • to provide appropriate information to prospective students • to make contact in case of school closure (e.g. adverse weather conditions) • to send SMS text messages and emails about meetings, etc.	Information required to confirm student/parent identity and contact through communications: • student name • gender • date of birth • family details (parents/guardians name, address, contact details to include phone numbers, email addresses etc).
2. Application information We use this to determine whether an applicant meets eligibility requirements as set out in our Admission Policy.	
In addition to data outlined at (1) above, we collect personal data via Application Forms and Student Transfer Forms. Where the student is offered a place, completed Application Forms are placed on the student's file. Where the student is not offered a place, the data will be used for the purposes of responding to any section 29 appeals process. Applicants may opt to provide data on "Religion" at this stage where this forms part of the school's admissions criteria. Any information not required to operate the Admissions Procedure, is identified as optional.	Information as required to ascertain eligibility under the school's Admissions Policy: • Name and address of current school • Class in current school • Details of siblings, etc. • Details of any special educational needs (SEN). • Language: details re Irish language. • Religion (based on consent)
3. Enrolment information Once the school has accepted the student's application, and has offered the student a place, other information is collected in addition to the data outlined at (1) and (2) above. This personal data is used for administrative and management tasks e.g. school communications, timetabling, scheduling parent teacher meetings, school events, arrangements for academic registration, class details, start dates, book lists, subject-selection, school trips etc.	
Contact and Identification Information: We use this information: • to make contact in case of school closure (e.g. adverse weather conditions), or an emergency (ill-health or injury), • to communicate issues relating to progress, welfare or conduct in school, non-attendance or late attendance, etc. • to send SMS text messages and emails about important events, e.g. start dates, course details, meetings, school events, etc.	• Student name and date of birth (requires birth certificate verification by school) • PPSN, Gender • Address including Eircode • Extended family details (parents/guardians name, address, contact details to include phone numbers, email addresses etc). • Details of next of kin (for contact in case of emergency)
Academic record: We use this information to deliver education appropriate to the needs of the student, to assess the student's educational progress. Standardised test results used for the purposes of assessing literacy/numeracy progress, for Reasonable Accommodation in State Examinations, for assisting in referrals to NEPS, and for career guidance etc.	• Reports, references, assessments and other records from any previous school(s) attended by the student. • Education Passport (6th Class Report provided by primary school after post-primary school confirms enrolment. Protocols set out in DES Circulars 42/2015 and 34/2016). • Standardised testing Results
Language spoken: Without this information the school will not know how to meet the student's needs and to deliver appropriate education. This ensures the student has access to language support (where necessary). Irish Exemption Information re application for Irish exemption if eligible (e.g. received primary school up to 11 years of age outside Ireland, evidence of disability, student from abroad etc).	• Information about language spoken (for language support) • Details of whether the student received EAL (English as an Additional Language) support. • Details re whether the student is exempt from studying Irish • Details to ascertain if student is eligible for exemption from study of Irish
Medical information for health purposes: This information is essential so that we can meet our duty of care to the student. We use this information to (i) ensure we know who to contact in case of an emergency, (ii) ensure that we have any relevant information to safeguard/prevent damage to the student's health (iii) meet the student's medical/care needs when they are in school (iv) facilitate appropriate advanced planning with parents/guardians (eg. notification to relevant personnel within	• Emergency contact details (name, telephone, details of relationship to the student etc). • Details of the student's GP (to be contacted in case of emergency). • Details of any relevant medical information (eg. medical condition, allergies, treatment/care plan etc) to facilitate appropriate advanced planning with parents/guardians. • This may include the use of the student's photograph for

the school, storage of medications, staff training where necessary etc).	display in the Staff room as part of the emergency action plan.
SEN and Medical information for educational purposes: We cannot meet our duty of care to the student and our obligations under EPSEN Act 2004 without this information. We use this information to (i) make application to the DES for allocation of resources to support student (ii) ensure school has relevant information to deliver education appropriate to student's needs (iii) apply for appropriate accommodation(s) and/or therapeutic supports where available.	• Details of any special needs/medical needs that need to be accommodated, e.g. medical assessment, psychological assessment/report. • Details of whether the student has been in receipt of learning support. • Details of whether the student been granted resource teaching hours and/or special needs assistance hours by the NCSE.
Information sought by Department of Education and Skills (DES): We are under a legal obligation to return specific enrolment information concerning each student to DES. This is used to calculate teacher and resource allocation, capitation, grant payments for schools, for statistical analysis and reporting in the areas of social inclusion and integration of students in the education system, and for planning purposes. The DES seeks some additional information on an optional basis (i.e. parental consent).	Personal data is transferred to the DES via the Post-Primary Online Database as set out in the Privacy Notice for P-POD provided by DES. Required information includes, e.g. mother's birth name (to verify student PPSN). Other (optional) information is sought for purposes relating to social inclusion and integration of students in the education system, and for planning purposes. • Whether the Pupil's mother tongue is English or Irish* • Ethnic/Cultural background*
Use of photographs for yearbooks, social media, website etc.: Photographs, and recorded images of students may be taken at school events and to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school.	• Consent to use (for these purposes) images or recordings in printed or digital format. • Separate consents will be sought for different publication forums. (NB This excludes CCTV recordings - see school CCTV policy).
Religion only sought where the school facilitates religious instruction/faith formation at the request of parent(s)/guardian(s).	• Religious denomination (based on consent)
Consents to direct marketing: If you wish to receive direct marketing you can give consent for us to contact you by SMS text and/or email. Your right to opt-out only relates to the school contacting you for direct marketing purposes.	Note: We will still contact you on your mobile in case of an emergency relating to your child and/or to communicate messages about school events (e.g. school closure, parent-teacher meetings etc).
4. Personal data gathered during student's time in School We cannot meet our statutory obligation to deliver appropriate education to students and/or we cannot satisfy our duty of care to each student without processing this information.	
Academic progress: The school processes this personal data in order to deliver education to students, and to evaluate students' academic progress, to register the student for State Examinations (Junior Cycle, Leaving Cycle), to submit the students' work to the recognised accrediting body etc.	• Academic progress and results • State exam results • Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results) • Continuous assessment and end of term/year reports
Attendance: The school is required to collect and monitor attendance data and to notify the Education Welfare Officer (TUSLA) in certain circumstances, such as (i) where the student is suspended for 6 days or more (ii) where the student is absent for an aggregate period of 20 school days during the course of the year, (iii) where the Principal is of the opinion that the student is not attending school regularly. The school will notify parent/guardian in the event of non-attendance or absences.	Statutory processing pursuant to the Education (Welfare) Act 2000. • Attendance records including Registers and Roll books etc. • Records of referrals to TUSLA Please note that the School Register and Roll Book are considered to be documents of enduring historical value. The School Register and Roll book are retained in the School's archives for archival purposes in the public interest.
School tours/trips: Information required to make appropriate travel arrangements, to implement insurance cover, to arrange appropriate supervision ratios, to ensure medical/health issues are properly accommodated, to engage in responsible planning, and to ensure necessary paperwork for INIS (Irish Border Control/Irish Naturalisation & Immigration Service requirements where children are travelling with someone other than their parent or guardian).	Information to ensure trip is properly organised and supervised, including: • permission slips (signed by parents/guardians), • itinerary reports • Letter from parent(s)/guardian(s) giving consent to travel. • Copy of birth or adoption certificate or guardianship papers • Copy of marriage/divorce certificate (where parent has different surname to child). • Copy of the parent/guardian's passport or State identity document.
Garda vetting outcomes: Certain work experience roles may	Information as set down in National Vetting Bureau (Children

require that a student be Garda vetted (Statutory vetting process).	and Vulnerable Persons) Act 2012. • Garda vetting form
CCTV images: The school processes this data for the purposes outlined in our CCTV Policy, a copy of which is available on the school's website e.g. *We use CCTV for security purposes; to protect premises and assets; to deter crime and anti-social behaviour; to assist in the investigation, detection, and prosecution of offences; to monitor areas in which cash and/or goods are handled; to deter bullying and/or harassment; to maintain good order and ensure the school's Code of Behaviour is respected; to provide a safe environment for all staff and students; for verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and the recordings may be capable of resolving that dispute; for the taking and defence of litigation.*	CCTV is in operation at the perimeter, exterior and certain internal common areas within the school both during the daytime and during the night hours each day. CCTV is used at external points on the premises (eg. at front gates, in the car-park etc) and at certain internal points (eg. front desk/reception area, corridors etc). In areas where CCTV is in operation, appropriate notices will be displayed.
Special needs data, educational support records, medical data etc: Without this information, the school will not know what resources need to be put in place in order to meet the student's needs and to deliver appropriate education in-keeping with its statutory obligations. This is in order to assess student needs, determine whether resources can be obtained and/or made available to support those needs, and to develop individual education plans. 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 (the statutory agency established under the Education for Persons with Special Educational Needs Act 2004) such information as the Council may from time to time reasonably request.	The school collects information relating to any special educational needs, psychological assessments/reports, information about resource teaching hours and/or special needs assistance hours, etc. Schools are also required to share this personal data with SENOs employed by the NCSE. • Psychological assessments, • Special Education Needs' files, reviews, correspondence • Individual Education Plans, • Learning support file, • Notes relating to inter-agency meetings, • Medical information (including details of any medical condition and/or medication/treatment required) • Psychological, psychiatric and/or medical assessments
Child protection, child welfare records: The school is required to follow DES Child Protection Procedures (Circular 81/2017) and to take appropriate action to safeguard the welfare of students in its care (Child Protection Procedures for Primary and Post-Primary Schools 2017). Staff have a legal responsibility to report actual or suspected child abuse or neglect to the Child & Family Agency ("TUSLA") and to An Garda Síochána. Mandatory reporting obligations arise under Children First 2015, the Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012.	Mandatory reporting obligations require data sharing with TUSLA, An Garda Síochána and any other appropriate law enforcement or child protection authorities. DES Inspectorate may seek access to the school's child protection records for audit purposes. • Child protection records • Child safeguarding records • Other records relating to child welfare • Meitheal meetings convened by TUSLA
Counselling & Pastoral Care Records: This information is required to provide access to counselling services and/or psychological services and to provide supports to students, resolve behavioural, motivational, emotional and cognitive difficulties through assessment and therapeutic intervention, to engage in preventative work etc. Personal data (and special category personal data) will be shared with third parties (e.g. TUSLA, NEPS, CAMHS, An Garda Síochána, Medical practitioners treating the student) for the purpose of the school complying with its legal obligations and/or in the student's vital/best interests.	• Guidance Counselling notes • Psychological service notes • Referrals to/records relating to therapeutic services and other interventions • Minutes, notes and other records concerning Student Support Team/Pastoral Care Team Meetings
Internal school processes: This information (e.g. anti-bullying processes and disciplinary/Code of Behaviour processes) is required to meet the school's duty of care to all its students and staff, to comply with relevant Circulars issued by the Department of Education and Skills, and to run the school safely and effectively. Data collected in these processes may be transferred to the school's insurer and/or legal advisors or management body as appropriate where required for disputes resolution, fact verification, and for litigation purposes.	• Records of parental complaints. • Records of other complaints (student to student complaints etc). • Records relating bullying investigations. • Records relating to Code of Behaviour processes (expulsion, suspension etc.) including appeals data and section 29 appeals material.
Accident and injury reports: This information is processed to operate a safe environment for students and staff, to identify and mitigate any potential risks, and to report incidents/accidents.	• Accident reports • Incident Report Forms • Notifications to insurance company

This data may be transferred to the school's insurance company and/or indemnifying body and/or legal advisors as appropriate. Data will be shared with An Garda Síochána, TUSLA and the Health & Safety Authority where appropriate.	• Exchanges with legal advisors. • Notifications to Health & Safety Authority (HSA)
Financial information, fees etc: Without this information, the school cannot process applications, make grant payments, or receive payment of monies (e.g. course fees, school trips etc). After completion of the payments, the documentation is retained for audit and verification purposes. The school's financial data are audited by external auditors.	• Information relating to payments from student's parents/guardians (including fee support and fee waiver documentation), • Scholarship/Grant applications (including Gaeltacht, book rental scheme etc).
5. Charity Tax Back Forms This information is required so that the school may avail of the scheme of tax relief for donations of money received.	
To claim the relief, the donor must complete a certificate and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. This information is retained by the School in the case of audit by the Revenue Commissioners.	• CHY3/CHY4 tax back forms • Donor name, Address & Telephone Number • PPS Number • Tax Rate • Signature • Gross amount of donation
6. Parent Nominees on Boards of Management This information is required to enable the Board of Management to fulfil its statutory obligations.	
Processing undertaken in accordance with the Education Act 1998 and other applicable legislation, including decisions taken for accountability and good corporate governance.	• Name, address and contact details of Parent Nominee • Records in relation to appointment to the Board • Minutes of Board of Management meetings and correspondence to the Board.

9 .Data Retention Schedule

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

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

Sensitive Personal Data Students	Final disposition	Comments
Professional reports	Never destroy	Archive when class leaves + 2 years, keep indefinitely
Special Education Needs' files, reviews, correspondence and Personal Pupil Plans/Individual Education Plans/Care Plans	Never destroy	Archive when class leaves + 2 years, keep indefinitely
Accident reports	Never destroy	Archive when class leaves + 2 years, keep indefinitely
Child protection records	Never destroy	Archive when class leaves + 2 years, keep indefinitely
Section 29 appeal records	Never destroy	Archive when class leaves + 2 years, keep indefinitely
Enrolment/transfer forms where child is not enrolled or refused enrolment	Two years	Confidential shredding
Records of complaints made by parents/ guardians	never destroy	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), then destroy

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.

Staff Records	Final disposition	Comments
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)

Staff personnel files (whilst in employment)	Final Disposition	Comments
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 (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)

Staff personnel files (whilst in employment)	Final Disposition	Comments
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 tobe 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.
Carer's 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
Other types of 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.
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	Confidential shredding	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.

Staff personnel files (whilst in employment)	Final Disposition	Comments
Grievance and Disciplinary records	Confidential shredding	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

Occupational Health Records	Final Disposition	Comments
		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		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

Promotion process	Final Disposition	Comments
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.

Principal / Deputy Principal appointment	Final Disposition	Comments
		• 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 unsuccessful 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.

10. Data Privacy Notices

10.1 When is a Data Privacy Notice required?

Where information is being collected directly from an individual, a Data Privacy Notice must be provided at the point at which the data is collected.

- Where information is obtained from another source, a Data Privacy Notice must be provided:

- If personal data is to be used to communicate with the data subject, at the latest at the time of the first communication with the data subjects;
- If disclosure to another recipient is envisaged, at the latest when personal data is first disclosed.

10.2 What needs to be included in a Data Privacy Notice?

Data Privacy Notice s must contain specific information which informs data subjects of:

- Who is collecting the data;
- Why it is being collected;
- What legal basis is being relied upon to process the data;
- How it will be processed;
- How long it will be kept for;
- Who it will be disclosed to.

11. Data Protection Communications

11.1 The Data Protection Policy

This document will be made known to all employees and staff as the primary source of Data Privacy Policy at Enable Ireland Sandymount School.

11.2 Enable Ireland Sandymount School Privacy Notice

Enable Ireland Sandymount School main method of informing data subjects and the general public regarding our use of their data is the Privacy Notice. The Privacy Notice will include at a minimum:

- Identification of Enable Ireland Sandymount School as the controller of personal information;
- A description of the personal information we hold and use;
- An explanation of what we use the information for;
- Who we share the information with;
- Where we store the information;
- How long we keep the information;
- A summary of the data subjects' rights as observed by Enable Ireland Sandymount School;
- Summary technical details regarding information processing (including cookie use);

The Data Privacy Notice will be formatted appropriately for the medium in which it is published.

The Data Privacy Notice is considered an advisory notice regarding Enable Ireland Sandymount School policy, and is not intended to constitute a contract with any person.

11.3 Enable Ireland Sandymount School Website Privacy Notice

Enable Ireland Sandymount School main method of informing data subjects and the general public regarding its use of their data whilst on our website will be the Website Privacy Notice. The Privacy Notice will include at a minimum:

- Identification of Enable Ireland Sandymount School as the controller of personal information;
- A description of the personal information we hold and use;
- An explanation of what we use the information for;
- Who we share the information with;

- Where we store the information;
- How long we keep the information;
- A summary of the data subject's rights as observed by Enable Ireland Sandymount School;
- Summary technical details regarding information processing (including cookie use);

The Data Privacy Notice will be formatted appropriately for the medium in which it is published.

The Data Privacy Notice is considered an advisory notice regarding Enable Ireland Sandymount School policy, and is not intended to constitute a contract with any person.

11.4 Data Privacy and employees

Employees and contractors will be formally notified of Enable Ireland Sandymount School position with respect to this policy via a staff briefing.

11.5 Communication plan for Privacy Notices

Enable Ireland Sandymount School will ensure that staff and external parties are informed regarding our use of their data. Any subsequent changes to our policy or practices which affect how user's data is processed will be communicated as per this section.

Employees will be informed directly by email informing of the change, and with attachments or links to supplementary information where required.

Enable Ireland Sandymount School main vehicle for informing the public of our privacy policy is the data privacy notice which is published on our website. This will be revised as necessary to ensure compliance.

Where certain classes of users (e.g. students) need to be informed more proactively regarding our use of their personal data, we will accomplish this by direct email to those users. This will be carried out in advance of the change going live. Where a change of use requires a response, the lack of a response will not be treated as acceptance.

From time to time it will be necessary to revise the Data Protection Policy as well as associated Privacy Notice in response to changes in regulations or evolution of expectations for compliance.

The data Privacy Notice itself contains an advisory to users to check regularly for changes.

12. Third Parties

12.1 General

Enable Ireland Sandymount School avails of the services of outside parties who act as Data Processors on our behalf to assist us in essential school processes.

These include but are not limited to software providers & IT contractors.

Enable Ireland Sandymount School will perform due diligence with respect to any and all such third parties and ensure that:

- The basis of the relationship is clearly defined and falls under Enable Ireland Sandymount School Data Protection Policy;
- A Data Processing Agreement is in place between our school and the third party that strengthens our compliance with the GDPR (appendix 5);

- Where data held may not come under GDPR, that a non-disclosure agreement protects personal data;

Only providers who are actively involved in processing personal data will come under scrutiny.

12.2 Transfers of personal data to non-EEA jurisdictions

Our use of third parties may include entities outside the EU/EEA who will process personal data of EU residents on our behalf in the direct exercise of our key school processes. Enable Ireland Sandymount School warrants that the use of non-EEA services is a school necessity. In these cases, Enable Ireland Sandymount School has identified the following:

Processor	Stored in the EU/EEA	EU/US Privacy Shield Agreement in place
Aladdin	yes	n/a
Host Ireland	yes	n/a
Instagram	yes	yes
Esinet	yes	n/a
Enable Ireland I.T. Department	Yes	n/a
Wiltshire Farm Foods	yes	n/a
FHM Accountants	yes	n/a
Zoom Video	yes	yes
Seesaw	yes	n/a
Instagram	yes	yes
Text-A-Parent (SMS service)	yes	n/a
Toptech Fire & Security	yes	n/a

13. Data Security Breaches

Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, Enable Ireland Sandymount School will give immediate consideration to informing those affected.

Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures.

In appropriate cases, Enable Ireland Sandymount School will also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, Department of Education etc.

If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, Enable Ireland Sandymount School may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to Enable Ireland Sandymount School as soon as the data processor becomes aware of the incident. (see appendix 3)

13.1 Risk Assessment

A detailed analysis of volumes and types of data involved will be undertaken and a risk assessment carried out to establish the risk to data subjects for every breach;

13.2 Notification

On the basis of the evaluation of risks and consequences, the Principal will decide whether it is necessary to notify relevant stakeholders i.e.

- the Gardaí;
- the Data Subjects affected by the breach;
- the Data Protection Commissioner;
- the School's Insurers;

In accordance with the Data Protection Commissioner's Code of Practice all incidents in which Personal Data has been put at risk will be reported to the Office of the DPC within 72 hours of the school first becoming aware of the breach.

If, following the assessment described above, it is established that the data breach has been fully and immediately notified to the Data Subjects affected and it does not include sensitive personal data or personal data of a financial nature, it may not be required to be notified to the DPC. This will be assessed on an individual basis according to the school's policy on Data Breach above, and where there is any doubt, legal advice will be sought.

13.3 Evaluation and Response

Following any serious Breach of Data incident, a thorough review will be undertaken by the response team and a report will be made to the Board of Management. This will identify the strengths and weakness of the process and will indicate what areas may need to improve.

Response may also include updating the Data Protection Policy and retraining staff

14. Subject Access Requests (SARs)

Enable Ireland Sandymount School recognises the right of data subjects to request information regarding data we hold on them.

14.1 Student making a Subject Access Request

A student aged eighteen years or older (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves;

If a student aged eighteen years or older has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student;

While a student aged from thirteen up to and including seventeen can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is our policy that:

- If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access;
- If the information is of a sensitive nature, parental/guardian consent will be sought before releasing the data to the student;
- If the information would be likely to be harmful to the individual concerned, parental/guardian consent will be sought before releasing the data to the student;

Each student request for Access to Personal Data will be assessed individually.

14.2 Parents/ Guardians making a Subject Access Request

Where a parent/guardian makes an access request on behalf of his/her child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the child, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the student is registered on the school's records and will be addressed to the student subject to the provisions above.

14.3 Subject Access Requests

The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of the processing of their personal data. Under the GDPR, individuals have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

- the reasons why their data is being processed,
- the description of the personal data concerning them,
- anyone who has received or will receive their personal data, and
- details of the origin of their data if it was not collected from them.

14.4 Logging Subject Access Requests

All requests received for access to or rectification of Personal Data must be directed to the Principal, who will log each request as it is received using the Subject Access Request Register. The data subject will be asked to fill out the Appendix 1: Subject Access Request Form.

14.5 Responding to Subject Access Requests

A response to each request will be provided within one calendar month (e.g. request received 2nd February should be issued by 2nd March) of the receipt of the written request from the Data Subject.

Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require Enable Ireland Sandymount School to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Enable Ireland Sandymount School cannot respond fully to the request within one calendar month, the school shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.

- An estimated date by which any remaining responses will be provided.
- The name and contact information of Enable Ireland Sandymount School individual who the Data Subject should contact for follow up.

14.5.1 Protecting Third Parties

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights. This redaction/withholding will be captured on the Schedule of Records (SOR).

15 Archiving Personal Data

Enable Ireland Sandymount School will archive personal data we hold for the purpose of retaining that data for no longer than it is outlined in the Data Retention section. Archiving will take place on an annual basis and will involve the following steps:

1. Identification of records (both electronic and paper) which contain personal data or sensitive personal data and their location (see Data Processing Map & Retention Policy in Section 8);
2. Identification of the purpose(s) for which the data was originally obtained i.e. why did we collect the data (see Data Processing Map & Retention Policy in Section 8);
3. The aim will be to consolidate the records relating to the data subject in one of two locations i.e. school drive on Enable Ireland's server & Archive (student records) or ESI-NET & Archive (staff records);
4. Appraisal of the records to determine if they contain personal data that a) should be retained for a certain period of time and disposed of or b) should be retained indefinitely for a specific lawful purpose (see Data Processing Map & Retention Policy in Section 8).
5. This step will involve:
    a. Consulting the Retention period as outlined in the Data Map & Retention Policy in Section 8.
    b. Identifying the records for disposal.
    c. Obtain permission from the Principal to dispose of the records.
    d. Document the disposal of records.
6. Once established, the data subject's files will be placed in an archive box and will be marked as "For Disposal DD/MM/YY" for records that will be retained for a specific time or "Archive Permanently" for records that will be retained indefinitely.
7. Consultation should also take place with the Principal for advice on record retention periods for certain records as needed.
8. Archived boxes will be held securely in the school's dedicated archive with restricted access.

16. Disposal of Personal Data

Enable Ireland Sandymount School will conduct a regular review of the personal data we hold for the purpose of disposing of redundant personal data. Such a review will take place on an annual basis and will involve the following steps:

1. Identification of records (both electronic and paper) which contain personal data or sensitive personal data (see Data Map & Retention Policy in Section 8);

2. Identification of the purpose(s) for which the data was originally obtained i.e. why did we collect the data (see Data Map & Retention Policy in Section 8);
3. Appraisal of the records to determine if they contain personal data which is no longer necessary for the purposes for which it was originally obtained: This step will involve:
   a. Consulting the Retention period as outlined in the Data Map & Retention Policy in Section 8.
   b. Identifying the records for disposal.
   c. Obtain permission from the Principal to dispose of the records.
   d. Document the disposal of records.
4. Suitable third-party service provider should be contacted to provide a secure erasure and destruction service i.e. confidential shredding through a certified data destruction specialist.
5. Consultation should also take place with the Principal for advice on record retention periods and to ensure that records are disposed of in a safe, secure and appropriate manner.

17 Governance framework

17.1 Supervisory Authority

The Irish Data Protection Commission is our lead supervisory authority under GDPR.

17.2 Monitoring Compliance

Enable Ireland Sandymount School will carry out internal GDPR compliance audits against school policy and procedures.

We will also arrange audits of our compliance by independent third parties at longer intervals.

All audit records will remain confidential to Enable Ireland Sandymount School and will be shown only to regulatory authorities on request. Each audit will, as a minimum, assess:

- Compliance with Data Protection Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities;
  - Raising awareness;
  - Training of Employees;
- • The effectiveness of Data Protection related operational practices, including:
  - Data Subject rights;
  - Personal Data incident management;
  - Personal Data complaints handling;
- The level of understanding of Data Protection Policies and Privacy Notices;
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.

The Data Protection Coordinator, in cooperation with key stakeholders will devise a plan with a schedule for correcting any identified gaps within a defined and reasonable time frame.

17.3 Disciplinary Procedure

Breaches of the GDPR or the school's Data Protection Policy may be treated as a matter for discipline and depending on the seriousness of the breach, and will be dealt with by the Principal in accordance with the School's Disciplinary Procedure.

For breaches of the GDPR Regulations, which do not warrant such action, the employee will be advised of the issue and given a reasonable opportunity to put it right.

In the case of contractors or external service providers, serious breaches of the policies and procedures can and will be deemed grounds for termination of contractual agreements.

Review and Ratification

This policy was reviewed and ratified by the Board of Management.

Signed: 

Sé Goulding, Chairperson of Board of Management

Jennifer Doyle, Principal

Date: 2 April 2025

Appendix 1

Data Access request form

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: (1 photographic id and one current proof of address)

- 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 procedure 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 license, 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

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.

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.

1. 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.

2. 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.

3. 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.

We do not transfer your personal data to a third country or international organisation.
We do not engage in automated decision making/profiling.

4. 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 section 8 Data Retention of our Data Protection Policy which is available on request from the School Office.

5. 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.

6. Contact

The Data Protection Officer (DPO) at Enable Ireland Sandymount School is the school principal and she can be contacted at sandymountschool.office@enableireland.ie

Appendix 3

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.

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.

1. 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.
2. Contact should be immediately made with the data processor responsible for IT support in the school.
3. In addition and where appropriate, contact may be made with other bodies such as the HSE, financial institutions etc.
4. 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.
5. 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.
6. 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.

7. 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.
8. 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.

Data Breach Action Plan

Identification and Initial Assessment of the Incident

- Identify and confirm volumes and types of data affected;
- Establish what personal data is involved in the breach;
- Identify the cause of the breach;
- Estimate the number of data subjects affected;
- Establish how the breach can be contained;

Recovery

- Establish who within the school needs to be made aware of the breach (DOP, BOM);
- Establish whether there is anything that can be done to recover the losses and limit the damage the breach could cause;
- Partial or complete systems lockdown;
- Establish if it is appropriate to notify affected individuals immediately (for example where there is a high level of risk of serious harm to any individual);

Risk Assessment

- A detailed analysis of volumes and types of data involved will be undertaken and a risk assessment carried out to establish and the risk to data subjects for every breach;

Notification

- On the basis of the evaluation of risks and consequences, the Principal will decide whether it is necessary to notify relevant stakeholders i.e.
  - the Gardaí;
  - the Data Subjects affected by the breach;
  - the Data Protection Commissioner;
  - the School's Insurers;
- In accordance with the Data Protection Commissioner's Code of Practice all incidents in which Personal Data has been put at risk will be reported to the Office of the DPC within 72 hours of the school first becoming aware of the breach.

- If, following the assessment described above, it is established that the data breach has been fully and immediately notified to the Data Subjects affected and it does not include sensitive personal data or personal data of a financial nature, it may not be required to be notified to the DPC. This will be assessed on an individual basis according to the school's policy on Data Breach above, and where there is any doubt, legal advice will be sought.

Evaluation and Response

- Following any serious Breach of Data incident, a thorough review will be undertaken by the response team and a report will be made to the Board of Management. This will identify the strengths and weakness of the process and will indicate what areas may need to improve.
- Response may also include updating the Data Protection Policy and retraining staff.

In summary:

Articles 33 and 34 of the General Data Protection Regulation 2016/679 state that reporting of breaches of personal data to the Data Protection Commission and to the affected data subjects are mandatory where the breach poses a high risk to data subjects.

Where reporting is required it must be done without delay and no later than 72 hours after having become aware of it.

This obligation should be reflected in appropriate contracts signed between data controllers and data processors also, so that a data processor processing on behalf of Enable Ireland Sandymount School will know to react immediately to any data breach that occurs through their processing, and report same to the Principal as soon as they become aware.

Any staff member who become aware of a data or a potential data breach are to report the breach to the Principal as soon as they become aware, who will then report to the Board of Management. The staff member reporting the breach will cooperate fully with the Principal in complying with the below steps and with any queries from the Data Protection Commission which may follow.

Staff may use the Data Breach Incident Report to report the potential data breach (Appendix 4)

Where it is determined together by the Principal and the Board of Management that the breach should be reported, the Principal will notify the Data Protection Commission, on behalf of the Board of Management as data controller, as follows:

Describe the nature of the breach, including the categories and approximate number of data subjects concerned, and the categories and approximate number of data records concerned;

Provide the Data Protection Commission with their name and contact details should more information be required;

Describe the likely consequences of the data breach; and

Describe the measures taken, or proposed to be taken by the Board of Management/School to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Appendix 4

Data Breach Incident Report

Data Breach Incident Report Form Data Breach Incident Number:			
Date and time of Incident:		Location of Incident:	e.g. email
Summary of Incident: (State facts only and not opinions. Please do **not** include identifiable information)			
Brief description of corrective actions taken			
Brief description of preventative actions taken			
Date and time Principal was informed			
Details of any further action taken by the Principal			
Reporter details			
Name: Job Role:		Email Contact Details:	Phone No:
Follow up details			
Investigations:			
Findings:			
Planned Actions:			
Principal sign off:		Date:	

Appendix 5

Data Processor Agreement

DATA PROCESSOR AGREEMENT DD/MM/YY

BETWEEN

(1) [The School]

Enable Ireland Sandymount School– "the Data Controller" and

(2) [The Service Provider]

Company

…… - "the Data Processor"

(3) Services provided by the company:

- **……**
- **……**

RECITALS

A. The Data Controller hereby appoints the Data Processor as its sub-contractor for the provision of specified services.

B. In order to perform the Services on the Data Controller's behalf, the Data Processor will require certain personal data to be made available to it by the Data Controller.

C. Under the Data Protection Acts 1988 and 2003, and any subsequent Data Protection legislation, the Data Controller is required to put in place an agreement between the Data Controller and any organisation which processes personal data on its behalf, governing the processing of that data.

D. The parties now wish to enter into this Agreement in order to regulate the provision and use of personal data that the Data Processor will be processing on behalf of the Data Controller.

AGREEMENT

1. DEFINITIONS AND INTERPRETATION

1.1 The following words and phrases used in this Agreement and the Schedules shall have the following meanings except where the context otherwise requires:

"Master Contract" means the main contract between the Data Controller and Data Processor setting out the terms and conditions for the services to be provided by the Data Processor.

"Data Subject" means an individual who is the subject of personal data;

"Personal Data" means data which relate to a living individual who can be identified from that data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller or Data Processor.

"Services" means the services to be carried out by the Data Processor under the terms of the Master Contract.

1.2 This Agreement shall continue in full force and effect for the same period as the Master Contract, unless terminated for breach by either party.

2. OBLIGATIONS OF THE DATA CONTROLLER

2.1 The Data Controller shall provide the personal data to the Data Processor together with such other information as the Data Processor may reasonably require in order for the Data Processor to provide the Services.

2.2 The instructions given by the Data Controller to the Data Processor in respect of the personal data shall at all times be in accordance with the laws of Ireland.

3. OBLIGATIONS OF THE DATA PROCESSOR

3.1 The Data Processor will process the personal data in compliance with the Irish Data Protection Acts 1988 and 2003, and Statutory Instrument 336 of 201 and any subsequent Data Protection legislation including General Data Protection Regulation GDPR of 2018.

3.2 The Data Processor undertakes that it shall process the personal data strictly in accordance with the Data Controller's instructions for the processing of that personal data, as outlined in Schedule 1.

3.3 The Data Processor will process the personal data for the following purposes only:
In order to provide the necessary managed services, as outlined in Schedule 1;

3.4 The Data Processor will treat the personal data, and any other Information provided by the Data Controller, as confidential, and will ensure that access to the personal data is limited to only those employees who require access to it for the purpose of the Data Processor carrying out the permitted processing and complying with its obligations under this Agreement.

3.5 The Data Processor will ensure that only such of its employees who maybe required by it to assist it in meeting its obligations under the Agreement shall have access to the personal data. The Data Processor will ensure that all such employees have undergone training regarding their data protection obligations, their duty of confidentiality under contract and in the care and handling of personal data.

3.6 The Data Processor agrees to assist the Data Controller promptly with all subject access requests which may be received from the Data Subjects of the personal data, so as to enable a response to the Data Subject within the maximum time permitted under law.

3.7 The Data Processor will not disclose the personal data to a third party in any circumstances other than at the specific written request of the Data Controller, unless the disclosure is required by law.

3.8 The Data Processor will NOT transfer the personal data outside of the European Union, other than with the specific written approval of the Data Controller.

3.9 The Data Processor will not sub-contract any of the processing without explicit written agreement from the Data Controller. Where such written agreement is provided, the Data Processor will ensure that any sub-contractor it uses to process the personal data complies with the terms of this agreement.

3.10 The Data Processor will employ appropriate operational and technological processes and procedures to keep the personal data safe from unauthorised use or access, loss, destruction, theft or disclosure. The organisational, operational and technological processes and procedures adopted are required to align with the requirements of ISO/IEC27001:2005 or a similar standard, as appropriate to the services being provided to the Data Controller. The Data Controller will use ISO/IEC27002:2005 as a basis for auditing compliance with the guarantees the Data Processor provides in relation to this obligation.

3.11 The Data Processor will not keep the personal data on any laptop or other removable drive or device unless that device is protected by being fully encrypted, and the use of the device or laptop is necessary for the provision of the services under this agreement. Where this is

necessary, the Data Processor will keep an audit trail of which laptops/drives/devices the personal data are held on.

3.12 The Data Processor will notify the Data Controller of any information security incident that may impact the processing of the personal data covered by this agreement within one working day of discovering, or becoming aware of any such incident. Following the report of the incident, the Data Processor will co-operate with the Data Controller's Compliance and Information Security procedures whilst they carry out a risk assessment, root cause analysis and identify any corrective action required. The Data Processor will cooperate with the Data Controller in implementing any required corrective action agreed between the parties.

3.13 On satisfactory completion of the service or on termination of this agreement, the Data Processor will ensure that the personal data is securely removed from their systems and any printed copies securely destroyed. In complying with this clause, electronic copies of the personal data shall be securely destroyed by either physical destruction of the storage media or secure deletion using appropriate electronic shredding software that meets international best practice. Any hard copy will be destroyed by cross-cut shredding and secure re-cycling of the resulting paper waste.

3.14 The Data Controller reserves the right, upon giving reasonable notice and within normal business hours, to carry out compliance and information security audits of the Data Processor in order to satisfy itself that the Data
Processor is adhering to the terms of this agreement. Where a sub-contractor is used, the Data Processor agrees that the Data Controller may also, upon giving reasonable notice and within normal business hours, carry out compliance and information security audits and checks of the sub-contractor to ensure adherence to the terms of this agreement.

4. THIRD PARTY RIGHTS

The Data Subject is hereby entitled to enforce the terms and conditions of this Agreement as a third party beneficiary.

5. INDEMNITIES

Each party shall indemnify the other against all costs, expense, including legal expenses, damages, loss, including loss of business or loss of profits, liabilities, demands, claims, actions or proceedings which a party may incur arising out of any breach of this Agreement howsoever arising for which the other party may be liable.

6. GOVERNING LAW

This Agreement shall be governed by and construed in accordance with Irish law and each party hereby submits to the non-exclusive jurisdiction of the Irish courts.

SIGNATURES

	Enable Ireland Sandymount School	**[The Service Provider]**
Name:		
Title:		
Date:		