



Stapolin Educate Together National School

Data Protection Policy

Introduction

This Data Protection Policy applies to the personal data held by Stapolin Educate Together National School ("the school") which is protected by the Data Protection Acts 1988 to 2018. The policy applies to all school staff, the Board of Management, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school) insofar as the measures under this Policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

Purpose of the Policy

The Data Protection Acts 1988 to 2018 and GDPR apply to the keeping and processing of Personal Data. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, students and their parents/guardians how their data will be treated.

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

1. be able to provide access to individuals to their data;
2. ensure it is held securely;
3. document our data protection procedures;
4. enhance accountability and transparency.

Data Protection Principles

The school Board of Management (BOM) is a data controller of personal data relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the BOM is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 which can be summarised as follows:

- **Obtain and process Personal Data fairly:** Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance

with the Data Protection legislation and the terms of this Data Protection Policy. The information will be obtained and processed fairly.

- **Consent:** Where consent is the basis for provision of personal data, (e.g. data required to join sports team/ after-school activity/ or optional school activity) the consent must be a freely given, specific, informed and unambiguous indication of the data subject's wishes. Stapolin ETNS will require a clear, affirmative action e.g. ticking of a box/ signing a document to indicate consent. Consent can be withdrawn in these situations.
- **Keep it only for one or more specified and explicit lawful purposes:** The School will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.
- **Process it only in ways compatible with the purposes for which it was given initially:** Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.
- **Keep Personal Data safe and secure:** Only those with a genuine reason for doing so may gain access to the information. Sensitive or 'Special Categories' of Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.
- **Keep Personal Data accurate, complete and up-to-date:** Students, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. Records must not be altered or destroyed without proper authorisation.
- **Ensure that it is adequate, relevant and not excessive:** Only the necessary amount of information required to provide an adequate service will be gathered and stored.
- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given:** As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of Personal Data relating to a student. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.

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

Definition of Data Protection Terms

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

- **Data** means information in a form that can be processed. It includes both automated data (e.g. electronic data) and manual data.
- **Relevant filing system** means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.
- **Personal Data** means data relating to a natural person who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller (BOM)
- **Sensitive or 'Special Categories' of Personal Data** refers to Personal Data regarding a person's:
 - racial or ethnic origin, political opinions or religious or philosophical beliefs;
 - membership of a trade union;
 - physical or mental health or condition or sexual life;
 - commission or alleged commission of any offence or
 - any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.
 - Biometric data (such as fingerprints)
 - Genetic data
- **Data Controller** - the Board of Management, Stapolin ETNS.
- **Data Subject** - an individual who is the subject of personal data.
- **Data Processing** means performing any operation or set of operations on data, including:
 - Obtaining, recording or keeping the data,
 - Collecting, organising, storing, altering or adapting the data,
 - Retrieving, consulting or using the data,
 - Disclosing the data by transmitting, disseminating or otherwise making it available,
 - Aligning, combining, blocking, erasing or destroying the data.

- **Data Processor** - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection legislation places responsibilities on such entities in relation to their processing of the data. Eg. Aladdin, Accountant etc.
- **Personal Data Breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This means any compromise or loss of personal data, no matter how or where it occurs

Rationale

In addition to its legal obligations under the broad remit of educational legislation, the school has a legal responsibility to comply with the Data Protection Acts 1988 to 2018 and the GDPR.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the Principal and Board of Management to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and Board of Management.

Other Legal Obligations

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

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education;
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School;
- Under section 20(5) of the Education (Welfare) Act, 2000, a Principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the Principal of another school to which a student is transferring. Stapolin ETNS may send a copy of school reports to the Principal of the new school the child has moved to. Where reports, which have been carried out by professionals, apart from Stapolin ETNS staff, are on current pupil files; such reports are only passed to another school following written permission having been sought and received from the parents of the said pupils.
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply Personal Data kept by it to certain prescribed bodies (the Department of Education

and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education);

- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers (“SENOS”)) such information as the Council may from time to time reasonably request;
- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be “personal data” as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body;
- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection
- Under *Children First Act 2015*, mandated persons in schools have responsibilities to report child welfare concerns to TUSLA- Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationship to the Characteristic ethos of the School

In line with our Educate Together ethos, Stapolin ETNS seeks to:

- enable students to develop their full potential
- provide a safe and secure environment for learning
- promote respect for the diversity of values, beliefs, traditions, languages, and ways of life in society.

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us.

Personal Data

The Personal Data records held by the school may include:

Staff Records:

A) Categories of staff data:

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

These staff records may include:

- Name, address and contact details, PPS number.

- Name and contact details of next-of-kin in case of emergency.
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave, etc.)
- Details of work record (qualifications, classes taught, subjects, etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under Children First Act 2015

B) Purposes:

Staff records are kept for the purposes of:

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

C) Location and Security Procedures of Stapolin ETNS:

- Manual records are kept in a secure, locked filing cabinet in a locked administration office only accessible to personnel who are authorised to use the data.
- Employees are required to maintain the confidentiality of any data to which they have access.
- Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office.
- The school has the burglar alarm activated during out-of school hours.

Student Records:

A) Categories of student data:

These may include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
 - name, address and contact details, PPS number
 - date and place of birth
 - names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
 - religious belief
 - racial or ethnic origin
 - membership of the Traveller community, where relevant
 - whether they (or their parents) are medical card holders
 - whether English is the student's first language and/or whether the student requires English language support
 - any relevant special conditions (e.g. special educational needs, health issues, etc.) which may apply
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student)
 - Psychological, psychiatric and/or medical assessments
 - Attendance records
 - Photographs and recorded images of students (including at school events and noting achievements).
 - Academic record – subjects studied, class assignments, examination results as recorded on official School reports
 - Records of significant achievements
 - Whether the student is exempt from studying Irish
 - Records of disciplinary issues/investigations and/or sanctions imposed
 - Other records e.g. records of any serious injuries/accidents, etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
 - Records of any reports the school (or its employees) have made in respect of the student to State Departments and/or other agencies under Children First Act 2015.

B) Purposes

The purposes for keeping pupil records includes:

- to enable each student to develop to his/her full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events, etc.
- to meet the educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to celebrate school achievements, e.g. compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the school's Photography Guidelines.

- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirement for attendance at Primary School.
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other schools, etc. in compliance with law and directions issued by government departments
- to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/references to second-level educational institutions.

C) Location and security procedures:

- Manual records are kept in a secure, locked filing cabinet/press in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.
- Digital records are stored on password-protected computer with adequate encryption and firewall software. The school has the burglar alarm activated during out-of-school hours.

Board of Management Records:

A) Categories of Board of Management Data:

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

B) Purposes:

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

C) Location and security procedures:

- Manual records are kept in a secure, locked filing cabinet/press in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.
- Digital records are stored on password-protected computer with adequate encryption and firewall software. The school has the burglar alarm activated during out-of-school hours.

Other Records: Creditors

A) Categories of Creditor Data:

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

- address
- contact details
- PPS number
- tax details
- bank details and
- amount paid

B) Purposes:

The purposes of keeping creditor records are:

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

C) Location and security procedures:

- Manual records are kept in a secure, locked filing cabinet/press in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.
- Digital records are stored on password-protected computer with adequate encryption and firewall software. The school has the burglar alarm activated during out-of-school hours.

Other Records: Charitable Donations

A) Categories of Donor Data:

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

- name
- address
- telephone number
- PPS number
- tax rate
- signature and
- the gross amount of the donation.

B) Purposes:

The purposes of keeping donor data:

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

C) Location and security procedures:

- Manual records are kept in a secure, locked filing cabinet/press in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.

- Digital records are stored on password-protected computer with adequate encryption and firewall software. The school has the burglar alarm activated during out-of-school hours.

Other Records: CCTV Images and Recordings

Stapolin ETNS does not currently have any CCTV cameras.

Other Records: Examination results

A) Categories of Examination Results Data:

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

B) Purposes

The main purpose for which these examination results are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardian about educational attainment levels and recommendations for the future. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and other schools to which pupils move.

C) Location and security procedures:

- Manual records are kept in a secure, locked filing cabinet/press in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.
- Digital records are stored on password-protected computer with adequate encryption and firewall software. The school has the burglar alarm activated during out-of-school hours.

Primary Online Database (POD) – Department of Education and Skills POD Privacy Statement

The General Data Protection Regulation (the GDPR) came into effect on the 25th May 2018. The GDPR applies across the European Union and aims to give individuals more rights, control and understanding of how their personal data is processed.

Under GDPR the Department of Education and Skills are required to keep you informed of the types of data we hold on you and your child, the purpose it is used for, and your rights in relation to how it is processed.

The Department of Education and Skills, which provides for the education and training of people resident in the State, requires certain personal data on all learners in order to fulfil its function. For primary school pupils, this data is held on the Primary Online Database (POD). The data held on POD forms the basis of the allocation of resources to schools as well as statistical reporting on education; it is also used for research and analysis into the operation of the education system and the formation of future policies. Data is shared with the Department of Employment Affairs and Social Protection for validation purposes, and with the Central Statistics Office under Section 31 of the Statistical Act for statistical reporting and analysis.

The complete Privacy Notice, which outlines further information in relation to the data held by the Department, can be found on the Department's website at the link below, as can full

details of the Department's data protection policy setting out how the Department will use your child's data, as well as information regarding your child's rights as a data subject.

<https://www.education.ie/en/TheDepartment/Data-Protection/>

If you have any further queries in relation to POD or the data held therein, the POD Helpdesk can be reached at 01 889 2311 or pod@education.gov.ie

Data Subject's Rights

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

Data subjects have a right to:

- (a) Request access to any data held about them by a data controller
- (b) Object to the processing of their personal data
- (c) Prevent the processing of their data for direct-marketing purposes
- (d) Ask to have inaccurate data amended
- (e) Data subjects have the right to complain to the Data Protection Commissioner
- (f) Data subjects have the right to be forgotten, or to require Stapolin ETNS to delete his or her personal data where that data is no longer needed for its original purpose, or where the processing is based on consent and the data subject withdraws that consent and no other lawful basis for the processing exists.
- (g) Where Stapolin ETNS has disclosed personal data to third parties, the data subject has the right to request information about the identities of third parties to whom his or her personal data have been disclosed.
- (h) Portability. A data subject may request a copy of his or her personal data in a commonly used machine-readable format, and to transfer it to another data controller.

Dealing with a Data Subject Access Request

Section 3 Access Request

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

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

Section 4 Access Request

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

- * The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- * Request must be responded to within 30 days
- * Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.

- * No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

Providing information over the phone

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

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

Data Processors:

Where the school uses a data processor off site, it is required by law to have a written contract in place (Third party agreement). This Third Party Agreement specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data must be deleted or returned upon completion or termination of the contract.

Personal Data Breaches

All incidents in which personal data has been put at risk must be reported to the Office of the Data Protection Commissioner within 72 hours except where the controller determines that “the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons”.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the BOM must communicate the personal data breach to the data subject without undue delay.

If a data processor becomes aware of a personal data breach, it must bring this to the attention of the data controller (BOM) without undue delay.

Retention of Records

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

In order to comply with this legal requirement, Stapolin ETNS has assigned specific responsibility and introduced procedures for ensuring that files are purged regularly and securely, and that personal data is not retained any longer than is necessary. See Appendix 1 and 2 below. All records will be periodically reviewed in light of experience and any legal or other relevant indications.

In all cases, schools should be aware that where proceedings have been initiated, are in progress, or are reasonably foreseeable (although have not yet been taken against the school/board of management/an officer or employee of the school (which may include a volunteer)), all records relating to the individuals and incidents concerned should be preserved and should under no circumstances be deleted, destroyed or purged. The records may be of great assistance to the school in defending claims made in later years.

In general, the limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim and the Statute of Limitations may be different in every case. In all cases where reference is made to “18 years” being the date upon which the relevant period set out in the Statute of Limitations commences for the purposes of litigation, the school must be aware that in some situations (such as the case of a student with special educational needs, or where the claim relates to child sexual abuse, or where the student has not become aware of the damage which they have suffered, and in some other circumstances), the Statute of Limitations **may not begin to run when the student reaches 18 years of age and specific legal advice should be sought by schools on a case-by-case basis**. In all cases where retention periods have been recommended with reference to the relevant statutory period in which an individual can make a claim, these time-frames may not apply where there has been misrepresentation, deception or fraud on the part of the respondent/defendant. In such a circumstance, the school should be aware that the claim could arise many years after the incident complained of and the courts/tribunals/employment fora may not consider the complainant to be “out of time” to make their claim.

Online Learning

While using online forums and platforms to facilitate learning and communication in our school, staff members are reminded that extra precautions need to be taken to avoid unintended data breaches.

- Staff members are only permitted to send documents containing personal data using their school email address.
- When emailing groups of parents/students/outside agencies, it is advisable to use the BCC function to avoid sharing email address with other people.
- Staff are reminded to avoid using personal or confidential data in the subject line of emails.
- Staff should only use approved devices, networks, cloud sharing sites, apps and programmes when working with children, parents and outside agencies.
- Staff are reminded that if using screen sharing functions, they must ensure that there are no unintended data breaches. They must ensure that only necessary windows are open on the screen and that they are signed in to any accounts prior to sharing their screen.
- Online meetings may only be recorded with the express permission of every attendee at the meeting.
- When working from home, staff are reminded of the importance of ensuring devices are password protected and kept safely.

Implementation Arrangements, Roles and Responsibilities

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

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

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

Monitoring the Implementation of the Policy

The implementation of the policy shall be monitored by the principal.

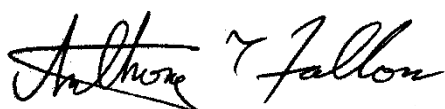
At least one annual report should be issued to the Board of Management to confirm that the actions/measures set down under the policy are being implemented.

Review and Evaluation

The policy will be reviewed and evaluated after 2 years. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or the NEWB), legislation and feedback from parents/guardians, students, school staff and others. The policy will be revised as necessary in the light of such review and evaluation and within the framework of school planning.

Ratification

This policy was ratified on 14th December 2020.



Signed: Anthony Fallon, Chairperson, Board of Management

Date: 14th December 2020

Appendix 1

The Records Retention Schedule for Stapolin ETNS (set out by dataprotectionschools.ie)

Records relating to pupils/students	Primary	Final Disposition	Comments
Registers/Roll books	Indefinitely	N/A	Indefinitely. Archive when class leaves + 2 years
Enrolment Forms	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority 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)
Student transfer forms (Applies from primary to primary; from one second-level school to another)	If a form is used- Student reaching 18 years + 7 years	Confidential shredding	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Disciplinary notes	Never destroy	N/A	Never destroy
Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results)	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority 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).
End of term/year reports	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority 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)
Records of school tours/trips, including permission slips.	Never destroy	N/A	Never destroy
Scholarship applications e.g.	Student reaching 18	Confidential shredding	18 is age of majority 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)

Records relating to pupils/students	Primary	Final Disposition	Comments
Gaeltacht, book rental scheme	years + 7 years		

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

Staff Records	Primary	Final disposition	Comments
<p>Recruitment process Note: these suggested retention periods apply to unsuccessful candidates only. They do NOT apply to successful candidates, or candidates who are/were also employees already within your school applying for another post/position. For successful candidates, or candidates who are/were also employees already within your school applying for another post/position, see retention periods set out below.</p>	✓	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 & CVs of candidates called for interview	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Database of applications	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Selection criteria	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Applications of candidates not shortlisted	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.

Staff Records	Primary	Final disposition	Comments
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)	Primary	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)

Staff personnel files (whilst in employment)	Primary	Final Disposition	Comments
Qualifications	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
References	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview: database of applications (the section which relates to the employee only)	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Selection criteria	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview board marking scheme & board notes	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Panel recommendation by interview board	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Recruitment medical	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Job specification/description	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Contract/Conditions of employment	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Probation letters/forms	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the

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

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

Occupational Health Records	Primary	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

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

Occupational Health Records	Primary	Final Disposition	Comments
			the school, plus 1 year for proceedings to be served on the school)

Superannuation /Pension /Retirement records	Primary	Final Disposition	Comments
Records of previous service (incl. correspondence with previous employers)	✓	N/A	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. 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	Primary	Final disposition	Comments
Any returns which identify individual staff/pupils,		N/A	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	Primary	Final disposition	Comments
Board agendas and minutes	✓	N/A	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	Primary	Final disposition	Comments
CCTV recordings	✓	Safe/secure deletion.	28 days in the normal course, but longer on a case-by-case basis e.g. where recordings/images are requested by An Garda Síochána as part of an investigation or where the records /images capture issues such as damage/vandalism to school property and where the images/recordings are retained to investigate those issues.
Financial Records	Primary	Final disposition	Comments
Audited Accounts	✓	n/a	Indefinitely
Payroll and taxation	✓		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	Primary	Final Disposition	Comments
Posts of Responsibility	✓	N/A	Retain indefinitely as it relates to pay/pension etc. (See DES guidelines)
Calculation of service	✓	N/A	Retain indefinitely
POR appeal documents	✓	N/A	Retain for duration of employment + 7 years (6 years in which to take a claim, plus 1 year to serve proceedings on school).
Correspondence from candidates re feedback	✓	N/A	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.

Appendix 2

Additional Data Protection Schedule For Stapolin ETNS

The BOM holds responsibility for the governance of the school's GDPR. The school, for the moment, is not required to appoint a Data Protection Officer, but the BOM authorises the Principal to function as an informal DPO while the BOM retains the governance liability.

Data Collected	Legal basis/Purpose	Storage/Access
Aladdin Schools	Aladdin is the school's official digital depository. A GDPR-compliant data processing agreement with Aladdin has been signed and is available on request.	Staff members should ensure not to divulge their Aladdin password to any other person, and passwords should not be stored by default on the class computer. Aladdin should be closed down when not in use, and when the room is unoccupied.
Teacher/Employee Data	The school holds teachers, SNA and all employee data on the Aladdin, DES's OLCS system and in hardcopy-files. The data collected refers to contact details/ records of leave, records of contracts, records of teaching/employment-history and are all necessary for the governance of the school in keeping with BOM governance protocols. On a voluntary basis the teachers may also have stored their bank details (for the purposes of remuneration and refund of expenses) and car insurance details (for the purposes of complying with DES regulations regarding use of staff cars for school business).	The Aladdin and OLCS systems are password protected. The hardcopy files are kept in locked cabinet in locked office. Records of contracts are kept for the duration of the teachers' employment and a further 7 years beyond that.
OLCS system	The Principal is an authorised approver of all data held on the DES's OLCS system	This access is specifically passworded for Principal only as approver, and for the deputy principal only as data-inputter.
Parent Association and associated parent groups.	The Parent Association may collect, on a voluntary basis, the names, addresses and contact details of volunteer members exclusively.	The Chairperson and Secretary of the PA are to ensure that access to this database/hardcopy is available only to the PA and used exclusively for the purpose of PA activity and no-other purpose. Similarly, for other parent groups.

Data Collected	Legal basis/Purpose	Storage/Access
Parents and other parents	At the beginning of each year parents are invited to be included in a class parent contact list. The list is shared only with those parents who have consented to be included in the list.	Other than this contact list the school does not share for any purpose any data from one parent to another (such as contact details etc.) and does not authorise any parent to construct a communication channel between any parents if such is done with reference to school-business.
Teacher Generated Documents	Any documentation generated by a teacher, or shared to the teacher by a parent, that refers to issues of medical nature, assessment reports, care/child-protection concern , school attendance should be given to the school Principal for storing/recording.	Kept indefinitely by school principal.
Teaching/Learning data and ICT	Teachers shall ensure not to cause or facilitate the children in inputting any data to third-party sources that are personal or identifying. For such ICT programmes the teacher should establish a coded or school-generated identity that will be deleted and disposed of once the programme has been completed. (e.g. Khan Academy etc.)	Acceptable Use Policy
Website and Social Media	The school's only formal social media presence is its website, and it has a prominent Privacy Statement.	No personal data for any person/child in the school community ever to be shared or posted.
BOM Documents	The BOM documents are stored securely. Hard copies of the minutes are stored in a locked cabinet.	The principal stores the BOM minutes in the locked filing cabinet in the office. These minutes are kept indefinitely.
BOM Confidentiality	All BOM members are obliged to observe confidentiality about matters discussed at BOM. Any documents distributed as part of BOM discussions should kept confidential. They may be returned at the end of the meeting and shredded.	All BOM members sign a Confidentiality Agreement at the beginning of their term on the BOM.

Data Collected	Legal basis/Purpose	Storage/Access
Financial records	The financial records of the school are also to be treated as confidential and should only be disclosed to the school's authorised accountant, the school's Patron, or as otherwise required by law.	The school's Financial records are stored in the office and annual financial reports to be stored indefinitely.
The BOM will on an ongoing basis approve research projects, public relations exercises and access to the school by student-teachers TY and SNA persons etc. which are of benefit to the school and in keeping with its commitment to its broader community.	The principal will inform the parents of any such projects or placements as they occur.	When engaging in these projects the principal will ensure the highest ethical standards apply and that there is no potential harm (and indeed a particular educational gain) or exposure to the child from engaging in these projects.
SNAs	SNAs may keep a journal for recording of incidents, observations and reflections but these entries are understood as aide memoires. Any important or ongoing concern as recorded in this aide memoire should be brought to the principal for formal discussion and recording. The SNAs journal should be stored securely and handed to the Principal at the end of the school year and stored securely and indefinitely.	Formal records on school templates and NCSE templates recorded by the SNA should be handed to the school Principal for storing and archiving. These records are kept indefinitely.
Tusla and Tusla authorised services, Gardai, Revenue Commissioners Department of Social Protection, Applications on foot of court order.	The school will comply fully with all requests from these statutory agencies.	
Family solicitors	Requests for school data from a family solicitor, whether via a parent, or independently delivered to the school, will be dealt with on a case by case and may involve legal advice or consultation with the National Data Protection Office.	

Data Collected	Legal basis/Purpose	Storage/Access
HSE and private health professionals	Any data requested by a Health Professional can only be released with the explicit permission by the child's parent.	
Community Organisations	Community organisation are not allowed to collect data from children on their visits to the school, nor will the school facilitate the sharing of any such data.	
Department of Education and Skills and DES officers	The DES is the Data Protection controller of the POD and OLCS systems and are responsible for any breaches of this data. The school complies with any exposure of data to the school's Inspectorate that may arise during school evaluation (e.g. access to IEPs, teacher-folders, anti-bullying index, child safeguarding index etc.)	