Knocknacarra Educate Together National School

Data Management and Data Protection Policy

This policy, which has been comprehensively reviewed by Knocknacarra ETNS, provides guidance for the maintenance of personal data in order to be compliant with the General Data Protection Regulation.

Contents

Introductory Statement:

At Knocknacarra Educate Together NS we aim to protect the well-being of our pupils, parents and staff by providing a safe, tolerant and caring environment. This policy endeavours to provide support to the school community regarding the management of data of a personal or sensitive nature.

This Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 and 2003 and is subject to the new requirements of the General Data Protection Regulation (GDPR).

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

Rationale:

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

The school takes its responsibilities under data protection law very seriously and wishes to put in place practices to safeguard individuals' 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.

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.

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education.
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School.
- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring.
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day.
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply personal data kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education

Welfare Board, the National Council for Special Education, other schools and 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 educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training).

- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers (SENOs)) such information as the Council may from time to time reasonably request.
- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body.
- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection or immunization administration.
- Under *Children First: National Guidance for the Protection and Welfare of Children* (2017), 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) and to maintain documentation according to the highest confidentiality standards.

Data Protection Terms:

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

Data means information in a form that can be processed. It includes both *automated data* (e.g. electronic data) and *manual data*. *Automated data* means any information on computer, or information recorded with the intention that it be *processed* by computer. *Manual data* means information that is kept/recorded as part of a *relevant filing system* or with the intention that it form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.

Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller i.e. the school.

Sensitive Personal Data refers to personal data regarding a person's

- racial or ethnic origin, political opinions or religious or philosophical beliefs,
- membership of a trade union,
- physical or mental health or condition or sexual life,
- commission or alleged commission of any offence or
- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

Data Controller for the purpose of this policy is the Board of Management of Knocknacarra ETNS. The principal, with the support of the secretary and other relevant staff members, manage the data. The principal, on behalf of the Board of Management, is the ***data protection officer***, acting as the point of contact for any data management queries. A ***data processor*** processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data during the course of his or her employment.

Data Protection Principles:

The school is a data controller of personal data relating to its past, present and future staff, students and parents/guardians. As such, the school is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 and the GDPR.

The GDPR identifies children as vulnerable persons deserving of specific protection. Children under the age of consent can never, themselves, give consent to the processing of their personal data. Enhanced individual rights under GDPR include:

- **The right to be informed** – This policy partially fulfils this requirement to provide fair processing information. In addition, privacy notices will be included on the online enrolment application as well as paper documentation used to gather data at the time of enrolment.
- **The right to access** – This policy provides clear processes for how data subjects may obtain confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the school shall provide a copy of the personal data, free of charge, in an electronic format.
- **The right to rectification** – Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If the school discloses personal data to third parties, which is limited solely to the Department of Education and Skills, the National Council for Special Education and professional

services such as therapists and psychologist as required and only after signed consent from parents, the school must inform them of the rectification where possible.

- **The right to be forgotten** – Also known as data erasure, the conditions for erasure include the data no longer being relevant to original purposes for processing or a data subject withdrawing consent. It should also be noted that this right requires the school to compare the subjects' rights to the public interest in the availability of the data when considering such requests. If an individual contacts the school and requests that their data be removed from its databases, it will be obliged to do so, unless it has a legitimate reason to retain the data.
- **The right to restrict processing** – In some situations, this right gives an individual an alternative to requiring data to be erased; in others, it allows the individual to require data to be held whilst other challenges are resolved. If personal data are 'restricted', then the school may only store the data. It may not further process the data unless the individual consents or the processing is necessary for establishment of legal claims, for the protection of the rights of another natural or legal person or for reasons of important public interest.
- **The right to data portability** – Data subjects may receive the personal data concerning them, which they have previously provided and have the right to transmit that data to another controller such as another school.
- **The right to compensation & liability data** – Subjects can sue both controllers and processors for compensation for pecuniary or nonpecuniary damage (e.g. damages for distress) suffered as a result of a breach of the GDPR.

The following practical guidelines apply:

- **Privacy by design:** The school will only collect data absolutely necessary for the completion of its duties (data minimisation). Access to personal data will be limited to those needing to act out the data processing. Before any protocols of this policy are changed, a Data Protection Impact Assessment shall be conducted where a type of processing is likely to result in a high risk to the rights and freedoms of individuals.
- **Obtain and process personal data fairly**: Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.
- **Keep it only for one or more specified and explicit lawful purposes**: The school will inform individuals of the reasons for data collection 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 personal data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely, and in relevant circumstances it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.
- **Keep personal data accurate, complete and up-to-date**: Students, parents/guardians and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. The principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.
- **Ensure that it is adequate, relevant and not excessive**: Only the necessary amount of information required to provide an adequate service will be gathered and stored.
- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given**: As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of personal data and sensitive personal data relating to a student. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.
- **Provide a copy of their personal data to any individual, on request**: Individuals have a right to know what personal data/sensitive personal data is held about them, by whom it is kept and the purpose for which it is held.

Personal Data Protocols:

Student records:

(a) **Categories of student data**:

- Information sought and recorded at enrolment, using paper forms, or which 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, including 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);
  - names and details for emergency contacts;
  - religious belief (with the option of parents to not consent);
  - racial or ethnic origin (with the option of parents to not consent);
  - membership of the Traveller community, where relevant (with the option of parents to not consent);
  - 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; and
  - 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 (see the Social Media and School Website Policy for relevant protocols)
- Academic record – class assignments, standardized test results, 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
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) **Purposes**: The purposes for keeping student records are:

- to enable each student to develop to their full potential;
- to comply with legislative or administrative requirements;

- to ensure that eligible students can benefit from the relevant additional teaching or financial supports;
- to 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;
- to use photographs and recorded images of pupils to celebrate school achievements, establish a school website, record school events and keep a history of the school;
- to facilitate the enrolment process;
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities; and
- to furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other schools in compliance with law and directions issued by government departments.

(c) **Location**: Manually stored, hard-copy data is stored in a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Each pupil has an individual folder for the storage of all documents.

Data is stored and managed using the Aladdin student management software. Aladdin processes personal data on behalf of the school in order to provide an online management information system. Aladdin is a secure software as a service application which is owned and run by Cloudware Ltd. (T/A Aladdin Schools), from where the data is only processed for supporting the purposes identified above. Aladdin and Google's security systems, used by Aladdin, are independently audited to international standards. Aladdin is security scanned daily and Google's data centre security is independently audited to ISO 27001, ISO 27017 and ISO 27018. For further information about Aladdin please visit: https://www.aladdin.ie/.

(d) **Security:** Manual records are kept in secure filing cabinets in the school office. Some documents may be temporarily written and stored by staff members in their classrooms. Anything of a confidential nature is stored securely.

The Aladdin cloud database uses the highest levels of encryption. Aladdin has systems to prevent unauthorized access including automatically logging out after a fixed period. Staff members use a username and password to access the Aladdin system and should adhere to and be aware of the following:

- Users are allocated different access rights to the Aladdin system. The access rights are solely determined by the school. At present, the principal is given full administrator rights.

The secretary is also an administrator but is not given access to information regarding academic progress. Mainstream teachers are given general access for their class only and are not granted administrative rights. Support teachers are given general access to all children as they work with multiple classes but not administrator rights.

- A log is taken of some actions undertaken by the user when using the Aladdin system and made available to the school.
- A unique username and password is provided to each user. Users should keep their username and password confidential and not disclose it to anybody or allow any person to access the system using their username and password. Staff members should change their passwords every 6 months and never store the passwords on any computers.
- The Aladdin system should only be used for the purposes of managing internal school administration activities and for no other purpose. The Aladdin system should not be accessed in the event of suspension or termination of the users' position at the school. The school is responsible for ensuring that access to the Aladdin system for terminated or suspended users is disabled.
- Each user should ensure they are familiar with the Aladdin system before use. All queries should be referred to the principal.
- The user should notify the Aladdin liaison person in the event of any misuse or loss of their username and password.
- The user should only login to the Aladdin system when in a secure and non-public environment, e.g. the school or home of the user.
- The user should sign out of the Aladdin system when leaving the device unattended.
- The Aladdin system should not be used to deal with emergency situations and it should not be relied upon during such times. Therefore, paper copies of emergency contact details are stored and locked in the secretary's desk as well as each teacher's desk.
- Users are responsible for ensuring that all communications sent to parents or guardians using the Aladdin system are accurate and are sent to parents/guardians for whom the school has appropriate and up to date consent and contact details.
- Before each communication, users should consult with the appropriate school's database to determine which parents or guardians have consented to being contacted.
- The Aladdin system should not be accessed through an unsecure network or internet connection. If in doubt, the user should wait until in a secure environment before accessing the Aladdin system.
- Information available through the Aladdin system should only be printed or saved to an electronic device where absolutely necessary. Any hardcopy or electronic files originating from the Aladdin system should be treated in accordance with the relevant provisions of this policy.

(e) **Retention Protocols:**

Student Records	**Retention**	**Final disposition**
Registers/Roll books	Indefinitely. Archive when class leaves + 2 years	N/A
Disciplinary notes	Never destroy	N/A
Records of school tours/trips, including permission slips	Never destroy	N/A
Enrolment forms	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)	Confidential shredding
Student transfer documentation		
End-of-term/year reports		
Results of in-school tests, including standardised test results	Actual test papers retained for one year. Results retained until a pupil is 18 (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).	

Sensitive Personal Data Students	**Retention**	**Final disposition**
Psychological assessments and other professional reports	Never destroy	N/A
Special education needs files including reviews, correspondence and Individual Education Plans		
Accident reports		
Child protection records		
Section 29 appeal records	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)	Confidential shredding
Enrolment/transfer forms where child is not enrolled or refused enrolment		
Records of complaints made by parents/ guardians	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 or other minor matter, then only until the student reaches 18 years + 7 years (6 years in which to take a claim, and 1 year for proceedings to be served on school)	Confidential shredding or N/A, depending on the nature of the records.

(f) **Additional protocols:**

- Parents can opt to have their contact details included in a class list of details shared with families as well as their contact details shared with the Parent-Teacher Association. Parents may revoke this consent at any time, though it must be acknowledged that once

contact details are shared, this revocation of consent only applies to future sharing of contact details.

- Communication with parents via emails is archived under password protection.

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 include:

- Name, address and contact details, PPS number;
- 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; and
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) **Purposes**: Staff records are kept for the purposes of:

- the management and administration of school business (now and in the future);
- facilitating 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);
- facilitating pension payments in the future;
- human resources management;
- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.;
- enabling 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);
- enabling 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**: In a secure filing cabinet located in the school office that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** A personal file for each staff member (past and present) is maintained for manual storage of the documents listed above as well as any other relevant data. Data related to recruitment processes is stored in specially created email accounts that are password-protected and follow ordinary encryption protocols. Any documents that are printed from applications are stored in a secure filing cabinet.

(e) **Retention Protocols:**

Staff Recruitment Records	Retention Timeframe	Final Disposition
Applications & CVs of candidates called for interview but were unsuccessful	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.	Confidential shredding
Candidates shortlisted but unsuccessful at interview		
Candidates shortlisted and are successful but do not accept offer		
Interview board marking scheme & board notes		
Panel recommendation by interview board		
Database of applications		Confidential shredding and/or deletion database
Selection criteria		
Applications of candidates not shortlisted		Deletion of associated email account
Unsolicited applications for jobs (typically for incidental subbing)	12 months from receipt of application	Confidential shredding

Staff Personnel Files	Retention Timeframe	Final Disposition
Application/CV	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).	Confidential shredding
Qualifications		
References		
Selection criteria		
Interview panel recommendation		
Recruitment medical		
Job specification/description		
Contract of employment		
Probation letters/forms		
POR applications and correspondence		
Leave of absence applications		
Job share		
Career Break		
Maternity/paternity leave		
Parental leave		
Force Majeure leave		

Carer's leave	Retain for 2 years following retirement or 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).	Confidential shredding
Working Time Act (attendance hours, holidays, breaks)	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).	
Allegations/complaints	Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served).	
Grievance and disciplinary records		

Occupational Health Records	**Final Disposition**	**Retention Timeframe**
Sickness absence records/certificates	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.
Pre-employment medical assessment		
Occupational health referral		
Correspondence re retirement on ill-health grounds		
Accident/injury at work reports		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).
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)	N/A	Indefinitely
Pension calculation	Confidential	Duration of employment + 7 years (6 years in which to

Pension increases Salary claim forms	shredding	take a claim against the school, plus 1 year for proceedings to be served on the school).

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

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 and
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular 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 decisions.

(c) **Location**: In binders/folders in a secure, locked cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Minutes and accounts are also stored on computers.

(d) **Security:** Manual records are kept in a locked, secure cabinet in the school office. All Board minutes and accounts files are password-protected. Minutes and accounts are distributed at meetings in hard-copy and collected at the end of the meetings to be shred. An agreed version

of the Board minutes, with any confidential sections removed, is included in the weekly newsletter and posted on the school website.

(e) **Retention Protocols:**

Board of Management Records	Retention Timeframe
Board minutes	Indefinitely.
Principal's monthly report including staff absences	Indefinitely. 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.

Financial Records	Retention Timeframe
Audited Accounts	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. Pay, taxation and related school personnel service records will be retained indefinitely. These records are kept on a computer system.
Invoices/back-up records/receipts	Retain for 7 years.

Charity Tax-back Forms

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

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

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

(c) **Location and Security**: Forms are kept in binder in a secure, locked cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

Department of Education and Skills Returns

(a) **Categories**: Upon enrolment, parents are requested to complete a form providing information to be shared with the Department through the Primary Online Database (POD). Information about POD is provided to parents in the form of an explanatory letter from the Department. Parents must provide specific consent to share sensitive data related to ethnicity and religious affiliation. The data will also be used by the DES for statistical, policy-making and research purposes. However, the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes. The DES has a data protection policy which can be viewed on its website (www.education.ie). The DES has also published a "Fair Processing Notice" to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (search for Circular Letter 0047/2010 in the "Circulars" section). In addition, until such time as the POD replaces the Annual October Census Return, at the beginning of each academic year the school submits an aggregate of information regarding the pupil enrolment that is not personal in nature.

(b) **Purpose:** POD allows the Department to maintain records on all pupils enrolled in national schools. It will in time deliver benefits to schools and parents by reducing form filling and allowing records to be transferred between schools automatically as a child moves school.

(c) **Location and Security**: Completed forms are filed and kept in a secure, locked filing cabinet that can be accessed only by authorized personnel. All information is added to the Aladdin system as well as POD via the OLCS website. Both databases provide robust encryption and are password protected. Employees are required to maintain the confidentiality of any data to which they have access.

Government returns	Final disposition	Comments
Any returns which identify individual staff/pupils	Confidential shredding or do not destroy.	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. POD, Annual Census, etc., keep in line with "Student Records" guidelines above.

Links to other policies

Relevant school policies already in place or being developed or reviewed shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

- Child Protection Policy
- Code of Behaviour and Anti-Bullying Policy
- Enrolment Policy
- Substance Use Policy
- Health and Safety Policy
- Social Media and School Website Policy

Processing in line with data subject's rights

Data will be processed in line with the data subjects' rights. Data subjects have a right to:

(a) Request access to any data held about them by a data controller

(b) Prevent the processing of their data for direct-marketing purposes

(c) Ask to have inaccurate data amended

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Dealing with Subject Access Requests

A 'subject access request' can be considered a data subject seeking information as to whether or not information concerning the subject is being processed and, usually, access to such data. The GDPR requires the provision of specific, additional information to data subjects when responding to access requests. The time period for dealing with requests is one month. While the school will not charge a fee for subject access requests, the school may charge a reasonable fee for any further copies requested by the data subject or where access requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information. The school is obliged to confirm the identity of any person making a 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 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)

- 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. 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 and
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Data Breaches:

A data breach occurs where the security or integrity of personal data is compromised. This can occur through misappropriation; loss or theft of data or equipment; unauthorised individuals gaining access; a deliberate attack on systems; equipment failure; human error or malicious acts such as hacking, viruses or deception. Breach notification is mandatory where a data breach is likely to result in a risk for the rights and freedoms of individuals. The principal, on behalf of the Board of Management, will notify parents or staff members without undue delay after first becoming aware of a data breach where there is a high risk, normally within 72 hours of being made aware of the breach. Normally this would include any personal data breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. The principal will document breaches, compiling the facts relating to the personal data breach.

Roles and Responsibilities:

In our school the board of management is the data controller and the principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

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

Individual	**Responsibility**

Board of management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

Monitoring the Implementation of Policy:

The implementation of the policy shall be monitored by the principal and the Board of Management. An annual report will be issued to the Board of Management to confirm that the actions/measures set down under the policy are being implemented.

Reviewing and Evaluating the Policy:

The policy should be reviewed and evaluated at least every three years and as necessary. On-going review and evaluation should 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 should be revised as necessary in the light of such review and evaluation and within the framework of school planning.

Ratification:

This revised policy was ratified by the Board of Management on the date below.

Date of Ratification: 8th March 2018