St Joseph's NS

Data Protection and Records Retention Policy

Updated May 2021

Introductory Statement

The review and update of this policy was formulated by the members of the Board of Management and staff in Saint Joseph's NS.

The school's Data Protection and Records Retention Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 and 2003.

This policy is a re-working of the policy using the template provided by the Data Protection in Schools website www.dataprotectionschools.ie. This website was developed by primary and post-primary management bodies with the assistance of the Department of Education and Skills.

The Records Retention Schedule is attached as Appendix 1 to this policy. The Personal Data Security Breach Code of Practice Template is attached as Appendix 2. The Personal Data Rectification/Erasure Request Form is attached as Appendix 3. The CCTV Policy template is attached as Appendix 4. The Enrolment Data Protection Statement is attached as Appendix 5.

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 and 2003.

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 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.

Scope

Purpose of the Policy: The Data Protection Acts 1988 and 2003 apply to the keeping and processing of *Personal Data*, both in manual and electronic form. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff and to inform staff, students and their parents/guardians how their data will be treated.

The policy applies to all school staff, the Board of Management, parents/guardians, students and others (including prospective or potential students and their parents/guardians, and applicants for staff positions within the school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

Data Protection Principles

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

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

- **Keep it only for one or more specified and explicit lawful purposes**: The School will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.

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

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

- **Keep Personal Data accurate, complete and up-to-date**: Students, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. The principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.

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

- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given**: As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.

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

Definition of Data Protection Terms

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

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

Other Legal Obligations

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

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education

- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School

- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring

- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day.

- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or

training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)

- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004,the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers "SENOs") such information as the Council may from time to time reasonably request

- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body

- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection

- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationships to the Characteristic Spirit of the School

Our Roman Catholic ethos aims to promote the full and harmonious development of all aspects of the person of the pupil - intellectual, physical, cultural, moral and spiritual. At St Joseph's NS **w**e aim to provide an environment where each child is given an opportunity to fulfil his/her potential in the academic, social, artistic, sporting and musical spheres. We recognise and value our rich traditional, rural heritage and our place in the history of the local community.

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us. The school wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection Acts.

Information Technology Security

St Joseph's NS uses the School's Broadband Programme which is managed by PDST Technology in Education, under the auspices of the Department of Education and Skills. It provides an integrated set of services to schools which includes broadband connectivity and hosted services including content filtering.

All staff desktops and the office PC are password protected using the Windows User Account Controls and password option. Encryption is used for portable devices such as the Principals laptop. Email communication referring to pupils or staff will be deleted within a timely manner, generally once a term, once the relevant issue has been addressed.

Personal Data

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

A ***Staff Records:***

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

- Name, address and contact details, PPS number
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

(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**:

- Secure, locked Staff filing cabinet: Individual Staff Files, Appointments files for shortlisted candidates.
- Secure, locked Office filing cabinet: Esinet/OLCS folder and records (for substitute teacher and SNA payments and teacher absences)

The Principal, Deputy Principal and School Secretary have authorised access to these files.

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

(d) Security:

- Individual hard copy personal files are stored in the secure, locked Staff filing cabinet.
- Where online applications are accepted they are received and stored on the password protected school

  email account
- Interview records for shortlisted candidates will be printed and stored in an Appointments Folder in the secure, locked Staff filing cabinet.

B ***Student Records:***

(a) **Categories of student data**: These **may** include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
  - name, address and contact details, PPS number
  - date and place of birth

- names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
- religious belief
- racial or ethnic origin
- membership of the Traveller community, where relevant
- whether they (or their parents) are medical card holders
- whether English is the student's first language and/or whether the student requires English language support
- any relevant special conditions (e.g. special educational needs, health issues,etc.) which may apply

- Information on previous academic record, including reports, references, assessments and other records from any previous school(s) attended by the student
- Psychological, psychiatric and/or medical assessments
- Child Protection/ Child Welfare Records
- Attendance records
- Photographs and recorded images of students (including at school events and noting achievements).
- Academic record – standardised test results as on official School reports
- Records of significant achievements
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

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

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

(c) **Location**:

- Secure, locked Pupil Filing Cabinet: Individual Pupil files
- Secure, locked Learning Support Cabinet: Individual Learning Support Pupil Files for relevant pupils.
- Secure, locked Child Welfare Filing Cabinet: Incidents Logbook, Anti-Bullying files, Child Protection files
- Secure and locked office Filing Cabinet: Current Enrolment Applications, Overall School Enrolment Folder
- Secure and locked Strong Room: Roll Book archive

- School Attic & Principals Office: Archive files for past pupils

The Principal, Deputy Principal and School Secretary have authorised access to these files.
Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security:

- These records will mainly be hard copy personal files in the locked Pupil Filing Cabinet and/or the Learning Support Pupil Filing Cabinet. Teachers will maintain one copy of the key for the Pupil Filing Cabinet in their room while another copy will be kept in the key box in the school office with each key coded appropriately.
- Pupil information for the Pupil Online Database (POD) will be generated in a Microsoft Excel Spreadsheet file. This file will be encrypted and password protected. The passwords will be made known to the Principal and Secretary only.

C B<u>oard of Management Records:</u>

(a) **Categories** of Board of Management data: These may include:

- 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 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 appointments and decisions.

Location:

- Secure, locked Principals Filing Cabinet.

The Principal and Staff Representative on the Board of Management will manage this access. Employees are required to maintain the confidentiality of any data to which they have access.

(c) Security:

- The Board of Management Meeting records are printed and stored in a Board of Management folder in the secure, locked Principals Filing Cabinet.
- Archive Board of Management folders are stored in the secure and locked strong room.
- The original electronic documents (e.g. minutes) are stored on the Principal's c drive. This file will be encrypted and password protected. The passwords will be made known to the Principal.
- Principal's reports emailed to the Board Recording Secretary for drafting as minutes of Boards meeting will be password protected and deleted once returned to the secretary of the Board.

D O<u>ther Records:</u>

C <u>reditors</u>

(a) **Categories of data**: the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):

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

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

(c) **Location**:

- Secure and locked Office Filing Cabinet:

The Principal, Deputy Principal and Secretary will manage this access. Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security:

- Manual record in Bank Payments folder stored in secure and locked Office Filing Cabinet.

E xamination/Assessment Records

(a) **Categories**:

- Individual Class Teachers will maintain an Assessment folder for their current class listing ongoing class assessments, e.g. weekly test results, teacher designed assessment tasks, portfolio material, etc.
- The school will hold data comprising annual standardised/screening assessment results in respect of its students
- An annual school report is issued for each student.

(b) **Purpose**: The main purpose for which these assessment results and other records are held is to monitor a student's progress. The data from the annual standardised test results is aggregated for statistical/reporting purposes and is transferred to the Department of Education and Skills each year via the online and secure Esinet system. Note: these are whole class reports and do not identify individual pupils.

(c) **Location**:

- Teacher's Desk: Class Based Assessment Folders.
- Secure, locked Pupil Filing Cabinet: Individual Pupil files, Copies of Annual Pupil Reports
- School Attic: Archive files for past pupils

For the annual standardised tests and annual reports, the Principal, Deputy Principal and School Secretary have authorised access to these files.

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

(c) Security:

1. Each Class Teacher and any visiting Department of Education and Skills Inspector requires access to the Class Based Assessment Folder. These folders are daily, working documents. They will be stored at the Teacher's Desk.
2. Other assessment records will mainly be hard copy personal files in the locked Pupil Filing Cabinet and/or the Learning Support Pupil Filing Cabinet.
3. Electronic Archive of previous Annual Pupil reports will be stored on the central, password controlled R drive on the school server. Electronic copies of these files must be deleted from all teachers laptops/PCs, from the "trash" folder and from any staff USB keys once the reports have been completed and stored in the central files.

Links to Other Policies and to Curriculum Delivery

Our school policies need to be consistent with one another, within the framework of the overall School Plan. During their review phase, 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
- Anti-Bullying Policy
- Code of Behaviour
- Enrolment Policy
- Substance Use Policy
- Acceptable Internet Use Policy
- Special Needs Policy
- Assessment Policy
- Promoting Positive Staff Relations Policy
- Health and Safety in The Workplace Policy

Processing in Line with Data Subject's Rights

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

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

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

(c) Ask to have inaccurate data amended

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

Dealing with a Data 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 40 days.
- A fee may apply but cannot exceed €6.35.
- 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.

Roles and Responsibilities

In our school the board of management is the data controller.

The Principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

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

Name	**Responsibility**
Board of Management:	Data Controller Principal: Implementation of Policy
Teaching personnel & relevant postholders:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality

Monitoring, Implementation and Review

The implementation of the policy shall be monitored by the Principal and a designated member of 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. This will be done in Term 3 each year. 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.

Ratification and Communication

This policy will be ratified by the Board of Management and will be implemented immediately after ratification.

When the Data Protection Policy has been ratified by the board of management, it becomes the school's agreed Data Protection Policy. The policy will be introduced to all staff and thereafter will be reviewed by the staff at the start of each school year

Notification of the availability of this and other school plans and policies is displayed on the Parents' Noticeboard and on the school web site.

A full copy of the policy will be made available on the school web site and parents will be informed that this is available.

The new Website Privacy Statement will be published on the school website immediately. At the point of enrolment, Parents/Guardians will be notified of the existence of the Data Protection Policy and informed where they can access it.

The plan was ratified by the Board of Management:on_____(date)

signed _____

Chairperson, Board of Management

Appendix 1

Retention of Records Schedule

Schools and ETBs 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 anonymized 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, Saint Joseph's NS has assigned specific responsibility and introduced procedures for ensuring that files are purged regularly and securely and that personal data is not retained any longer than is necessary. All records will be periodically reviewed in light of experience and any legal or other relevant indications.

IMPORTANT: 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.

WARNING: 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 Statue 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/ETB 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.

Student Records	Primary	Comments
Registers/Roll books	Indefinitely	Indefinitely. Archive when class leaves + 2 years
State exam results	N/A	SEC responsibility to retain, not a requirement for school/to retain.

Records relating to pupils/students	Primary	Confidential shredding	Comments
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, itinerary reports	Never destroy	N/A	Never destroy
Scholarship applications e.g. Gaeltacht, book rental scheme	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)
Garda vetting form & outcome - **STUDENTS**	N/A **as primary schools pupils will not be undergoing vetting**	Confidential shredding	Record of outcome retained for 12 months. School to retain the reference number and date of disclosure on file, which can be checked with An Garda Siochana in the future.

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	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
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.		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.
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)
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)

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)
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)
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)
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)
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)
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)

Probation letters/forms		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
POR applications and correspondence (whether successful or not)		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Leave of absence applications		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Job share		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Career Break		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Maternity leave		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)

Paternity leave		Confidential shredding	Retain for 2 years following retirement/resignation or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).
Parental leave		Confidential shredding	Must be kept for 8 years - Parental Leave Act 1998 Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years.
Force Majeure leave		Confidential shredding	Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years.
Carers leave		Confidential shredding	Must be kept for 8 years - Carer's Leave Act 2001 Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years.
Working Time Act (attendance hours, holidays, breaks)		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school). There is a statutory requirement to retain for 3 years
Allegations/complaints			Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). **Please note** the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains “active” on an employee’s record.
Grievance and Disciplinary records			Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). **Please note** the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains “active” on an employees’ record.

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

Superannuation /Pension /Retirement records	**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 agenda 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.
Principal's monthly report including staff absences		N/A	Indefinitely. Administrative log and does not relate to any one employee in particular: the monthly reports are not structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Not a "relevant filing system".

Financial Records	Primary	Comments
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. 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 on master file as it relates to pay/pension etc. (See DES guidelines)**
Calculation of service	☐	N/A	Retain indefinitely on master file
Promotions/POR Board master files	☐	N/A	Retain indefinitely on master file
Promotions/POR Boards assessment report files	☐	N/A	Retain original on personnel file in line with retention periods in "Staff Records" retention guidelines above
POR appeal documents	☐	N/A	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	☐	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
Personal Data Security Breach Code of Practice

Purpose of Code of Practice This Code of Practice applies to the Board of Management of St Joseph's N.S. as data controller [1]

This Code of Practice will be:

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

Obligations under Data Protection

The school as data controller and appropriate data processors so contracted, are subject to the provisions of the Data Protection Acts, 1988 and 2003 and GDPR and exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

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

Protocol for action in the event of breach

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

1. The school will seek to contain the matter and mitigate any further exposure of the personal data held. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, laptops, networks etc. and requesting that staff do not access PCs, laptops, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.
2. Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011. The penalties for withholding information include a fine of up to €5,000- or 12-months' imprisonment on summary conviction.
3. Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the school may conclude that there is no risk to the data and therefore no need to inform data subjects or contact the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.
4. Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (2) above.
5. Contact should be immediately made with the data processor responsible for IT support in the school.
6. In addition, and where appropriate, contact may be made with other bodies such as the HSE, financial institutions etc.
7. Reporting of incidents to the Office of Data Protection Commissioner: All incidents in which personal data (and sensitive personal data) has been put at risk shall be reported to the Office of the Data Protection Commissioner as soon as the school becomes aware of the incident (or within 2 working days thereafter), save in the following circumstances:

   When the full extent and consequences of the incident have been reported without delay directly to the affected data subject(s) and

   - The suspected breach affects no more than 100 data subjects and

[1] Unless otherwise indicated, terms used in this Code – such as "personal data", "sensitive personal data", "data controller", "data processor" – have the same meaning as in the Data Protection Acts, 1988 and 2003 and GDPR.

- It does not include sensitive personal data or personal data of a financial nature[2]

8. The school shall gather a small team of persons together to assess the potential exposure/loss. This team will assist the Principal of the school (and the school's DP Compliance Officer) with the practical matters associated with this protocol.
9. The team will, under the direction of the Principal, give immediate consideration to informing those affected[3]. At the direction of the Principal, the team shall:
   - Contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.
   - Where possible and as soon as is feasible, the data subjects (i.e. individuals whom the data is about) should be advised of
     - the nature of the data that has been potentially exposed/compromised;
     - the level of sensitivity of this data and an outline of the steps the school intends to take by way of containment or remediation.
   - Individuals should be advised as to whether the school intends to contact other organisations and/or the Office of the Data Protection Commissioner.
   - Where individuals express a particular concern with respect to the threat to their personal data, this should be advised back to the principal who may, advise the relevant authority e.g. Gardaí, HSE etc.
   - Where the data breach has caused the data to be "damaged" (e.g. as a result of hacking), the principal shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.
   - The principal shall notify the insurance company with which the school is insured and advise them that there has been a personal data security breach.

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

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

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

[2] 'personal data of a financial nature' means an individual's last name, or any other information from which an individual's last name can reasonably be identified, in combination with that individual's account number, credit or debit card number.

[3] Except where law enforcement agencies have requested a delay for investigative purposes. Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows. Where St Paul's N.S. receives such a direction from law enforcement agencies, they should make careful notes of the advice they receive (including the date and the time of the conversation and the name and rank of the person to whom they spoke). Where possible, St Paul's NS should ask for the directions to be given to them in writing on letter-headed notepaper from the law enforcement agency (eg. An Garda Siochána), or where this is not possible, St Paul's N.S. should write to the relevant law enforcement agency to the effect that "we note your instructions given to us by your officer [insert officer's name] on XX day of XX at XXpm that we were to delay for a period of XXX/until further notified by you that we are permitted to inform those affected by the data breach."

- the action being taken to limit damage or distress to those affected by the incident a chronology of the events leading up to the loss of control of the personal data; and
- the measures being taken to prevent repetition of the incident.

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

Appendix 3

The Personal Data Rectification / Erasure Request Form

Request to have Personal Data rectified or erased.

Data Protection Act 1988 and Data Protection (Amendment) Act 2003

Important: Proof of identity (eg. official/State photographic identity document such as drivers licence, passport) must accompany this form.

Full Name:	
Address:	
Contact Number:	Email Address:

Please tick the box which applies to you:

Student Staff ☐

Student ☐	Parent / Guardian of a Student ☐	Former Student ☐
Age:	Name of Student:	Insert Year of Leaving:
Year Group/ Class:		

Current Staff ☐	Former Staff ☐
Insert Years From / To:	Insert Years From / To:

I, ……[insert name] wish to have the data detailed below which ……[Name of School/centre] holds about me/my child rectified / erased (delete as appropriate). I am making this access request under Section 6 of the Data Protection Acts.

Details of the information you believe to be inaccurate and rectification required OR reason why you wish to have data erased:

You must attach relevant documents as proof of correct information e.g. where a date of birth is incorrect, please provide us with a copy of the official State Birth Certificate. Please note that your right to request rectification/deletion is not absolute and may be declined by St Joseph's NS in certain cases. You have the right to complain this refusal to the Office of the Data Protection Commissioner: see www.dataprotection.ie .

Signed…… Date ……

Checklist: Have you:

1) Completed the Access Request Form in full?

2) Included document/s as proof of correct information?

3) Signed and dated the Request Form?

4) Included a photocopy of official/State photographic identity document (driver's licence, passport, etc.) *

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

Appendix 4

CCTV & Data Management Policy

A Closed Circuit Television System (CCTV) is installed in St. Joseph's N.S. under the remit of the Board of Management.

Purpose of the Policy

The purpose of this policy is to regulate the use of CCTV and its associated technology in the monitoring of the environs of premises under the remit of the Board of Management of St. Joseph's N.S.

Purpose of the CCTV System

The CCTV system is installed internally and externally on the premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation to deter crime, vandalism, theft, and bullying, as an aid to the promotion of high-quality Health and Safety standards and to the discharge of the school's duty of care within and/or in the external environs of the premises at all times.

Scope of this policy

This policy applies to all staff, pupils, and visitors to St Joseph's N.S. It relates directly to the location and use of CCTV, the monitoring, recording and subsequent use of such recorded material.

General Principles

The Board of Management of St Joseph's N.S, as the corporate body, has a statutory responsibility for the protection of the school property and equipment as well as providing a sense of security to its employees, students and invitees to its premises. St Joseph's N.S owes a duty of care under the provisions of Health, Safety and Welfare legislation and utilises the CCTV system and its associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life in St Joseph's N.S by integrating the best practices governing the surveillance of its premises.

The primary aim of the CCTV system in St Joseph's N.S is to deter crime and vandalism and to assist in the protection and safety of the said property and its associated equipment and materials.

Monitoring for security purposes will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies and personnel for other purposes is prohibited by this policy.

Information obtained through video monitoring may only be released when authorised by the Principal, following consultation with the Chairperson of The Board of Management.

CCTV monitoring of public areas, for security purposes, will be conducted in a manner consistent with all existing policies adopted by the Board of Management including the provisions set down in Equality and other Education related legislation.

The industry code of practice for video monitoring prohibits monitoring based on the classifications contained in Equality and other related legislation e.g. gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of the Traveller community.

Video monitoring of public areas, for security purposes, within St. Joseph's N.S. is limited to areas that do not violate the reasonable expectation to privacy as defined by law.

Data from the CCTV system will be accessed and used in accordance with Data Protection Regulations.

Cameras are located in the following areas:

Internal

- The Reception/Lobby Area
- All Ground Floor Corridor Areas
- Upper Floor Corridor Areas

External

- The Main Entrance Area
- At/on the soffits of all external wall areas covering points of entrance/exit, Yard Areas, and Perimeter Fencing.

Signage is erected at the school entrance advising that a CCTV System is in operation in at the school. The signage includes the name and contact details of the data controller as well as the specific purpose for which the CCTV cameras are in place.

Staff, pupils and parents/guardians are informed of the location and purpose of the CCTV system as outlined above. The right to access images captured by CCTV cameras shall be in accordance with the Data Protection Acts of 1998 and 2003, and as per St Joseph's N.S Data Protection Policy.

Data Protection

All personal data recorded and stored by the CCTV system is governed by the Data Protection Acts of 1998 and 2003. Under the Data Protection Acts a data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information in manual files or in a computerised

form. The data controller in respect of images recorded and stored by the CCTV system in the school is the Principal on behalf of the Board of Management.

The personal data recorded and stored by the CCTV system will only be available to the data controller and will be used only for the purposes outlined in this Policy.

Individuals whose images are recorded and stored by the CCTV system shall have the right to request and receive a copy of personal data processed by the system. Such requests shall be made in writing to the data controller and shall be complied with within a maximum of 40 days. Personal data recorded by the CCTV system shall be retained for a maximum of 31 days. Thereafter it will be deleted automatically.

The recorded footage and the monitoring equipment shall be securely stored in the Principal's and Secretary's Office area. Unauthorised access to those Offices is not permitted at any time. The Offices are secured by means of the Access Control System.

The following procedures shall be followed in the event that An Garda Síochána seeks to view or take a copy of CCTV footage from the school's CCTV systems:

1. The data controller shall satisfy himself/herself that there is an investigation underway
2. A request from An Garda Síochána must be made in writing on Garda Síochána headed notepaper.

All CCTV systems and associated equipment are required to be compliant with this Policy.

Responsibilities:

The ***Board of Management*** will:

- Ensure that the CCTV Policy is in place, compliant with relevant legislation, to govern the use of CCTV in the school
- Ensure this Policy is reviewed regularly by the Board of Management.

The ***Principal*** will:

- Act as Data Controller on behalf of the Board of Management
- Ensure that the use of the CCTV system is used in accordance with this Policy as set down by the Board of Management
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the school
- Ensure that all CCTV monitoring systems are compliant with this Policy
- Be responsible for the release of any information or material in compliance with this Policy
- Maintain a record of the release of any material recorded or stored on this system
- Provide a list of the CCTV cameras, their locations and the associated monitoring equipment and the capabilities of such equipment to the Board of Management for formal approval
- If required, approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events
- Ensure that all areas being monitored are not in breach of a reasonable expectation of the privacy of individuals within the school
- Advise the Board of Management to ensure that adequate signage, at appropriate and prominent locations, is displayed
- Ensure that external cameras are not intrusive in terms of their positions and views of residential housing and comply with the principle of 'reasonable expectation of privacy'

- Ensure that recorded material is retained for a period not longer than 31 days and will be erased unless required as part of a criminal investigation or court proceedings, criminal or civil, or other bona fide use as approved by the Board of Management
- Ensure that monitors are stored in a secure place with access by authorised personnel only.

Links to Other Policies and to Curriculum Delivery

All school policies are consistent with one another, within the framework of the overall School Plan. Relevant school policies already in place, being developed or reviewed, are examined with reference to the CCTV Policy and any implications which it has for them are addressed.

The following policies are among those considered:

- Data Protection Policy
- Child Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Mobile Phone Code
- ICT Acceptable Usage Policy

The CCTV Policy has been developed mindful of the school's obligation under Data Protection Legislation.

Implementation Arrangements, Roles and Responsibilities

The School Principal is assigned the role of co-ordinating implementation of this CCTV Policy and for ensuring that all members of the school community are familiar with the Policy.

Ratification & Communication

A draft CCTV Policy was developed by the staff of Saint Joseph's NS. This draft Policy was circulated to all staff and BoM members and to the officers of the PFA for review and comment. The Committee finalised the draft Policy having regard to the feedback received. The BoM reviewed the draft Policy and the CCTV Policy was ratified by the BoM at its meeting on May 17th 2021.

The ratified Policy was circulated by email to all staff members and to the officers of the PFA. All parents were advised of the availability of the Policy on the school website at www.stjosephskilcock.ie and of the availability of a hard copy of the Policy for perusal through the Secretary's Office. Staff members are required to be familiar with the CCTV Policy.

Implementation Date

Implementation of the Data Protection Policy commenced with effect from 17th May 2021.

Monitoring the implementation of the Policy

Staff and the Board of Management members will satisfy themselves on an on-going basis that the actions/measures set down under the Policy are being implemented.

Reviewing and evaluating the Policy

Ongoing review and evaluation of this Policy 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.

Practical indicators that will be used to gauge the impact and effectiveness of the policy will include the extent to which:

- Students, staff and parents/guardians are aware of the policy
- Requests for access to personal data are dealt with effectively
- Personal data records are held securely
- Personal data records are retained only for as long as necessary.

Appendix 5

Enrolment Data Protection Statement

Applicants should be aware that section 66(6) of the Education (Admission to Schools) Act 2018 allows for the sharing of certain information between schools in order to facilitate the efficient admission of students.
Section 66(6) allows a school to provide a patron or another board of management with a list of the students in relation to whom—

(i) an application for admission to the school has been received,

(ii) an offer of admission to the school has been made, or

(iii) an offer of admission to the school has been accepted.

The list may include any or all of the following:

(i) the date on which an application for admission was received by the school;

(ii) the date on which an offer of admission was made by the school;

(iii) the date on which an offer of admission was accepted by an applicant; 8

(iv) a student's personal details including his or her name, address, date of birth and personal public service number (within the meaning of section 262 of the Social Welfare Consolidation Act 2005).