



St Joseph's Adolescent School
Roll No. 20153N

Data Protection Policy

Introductory Statement

The school's Data Protection Policy applies to the personal data held by the school, and is subject to the Data Protection Acts 1988, 2003, and the General Data Protection Regulation (GDPR).

The policy applies to all school staff; the board of management; the MDT; students and their parents/guardians; and applicants for staff posts within the school. Data is 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

St Joseph's Adolescent 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. School policy procedures are as follows:

- **Obtaining and process personal data fairly:**

Student information is gathered with the help of the MDT, consenting parents/guardians, and the student's respective school staff. All information is furnished by the individuals with full and informed consent. 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.

- **Keeping it only for one or more specified and explicit lawful purposes:**

Individuals have a right to know what personal data is held about them, by whom, and the purpose for which it's held. Thus, staff will explain to individuals why they collect their data when asked. Information is sought with the best interest of the individual in mind at all times.

- **Processing data 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 same will be strictly controlled.

- **Requesting data:**

If a student, parent/guardian, employee or former employee requests their personal data, the original document or a scanned copy thereof must be relinquished by the Principal or appropriate personal in St. Vincent's Hospital, Fairview. The Principal has 1 calendar month to provide this, without exception, beginning from the date of request.

- **Keeping personal data safe and secure:**

Only those with a genuine reason for doing so may gain access to information. Sensitive personal data is securely stored in manual records under lock and key. Firewall software and password protection is used to safeguard electronically stored data.

- **Keeping personal data accurate, complete and up-to-date:**

Where necessary, students, parents/guardians, and staff are obliged to add to staff and student records to keep information updated. The Principal may delegate such tasks to another member of staff. If an alteration 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.

- **Retaining data:**

Student information is retained until the student is aged 18 + 2 years. Information on staff is retained for the full duration of their tenure at the school. Information on unsuccessful staff applicants is retained for a maximum of eighteen months.

- **Destroying data:**

Two shredders are in the school – one in the Principal's office and one in the main office. Data, which is no longer required, will be shredded at the school and/or disposed of through the *SVHF Shredding Procedure*. *Same displayed in main office.

Scope

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

The policy applies to all school staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians, and

applicants for staff positions within the school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

Definition of Data Protection Terms

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

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

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

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

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 the school.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, St Joseph's Adolescent 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.

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 students attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection
- Under Children First: National Guidance for the Protection and Welfare of Children (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationship to characteristic spirit of the School (School's mission/vision/aims)

St Joseph's Adolescent School seeks to

- enable the full and harmonious development of all aspects of the individual student
- provide a safe and secure environment for learning
- promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society.

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

Personal Data

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

A. Staff records:

- (a) **Categories of staff data:** As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:
- Name, address and contact details, PPS number
 - 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).
- Garda Vetting reports
- Medmark Occupational Health reports and other medical certificates certifying absences from school for medical reasons.

(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:** Staff records are kept in a secure, locked filing cabinet in the Principal's Office that only personnel who are authorised to use the data can access. Electronic copies of staff records are kept on the Principal's Computer and maintained with firewall and password protection. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** These files are maintained in a locked filing cabinet and the Principal's computer in the Principal's Office in the school. Access is through the school Principal. Staff have access to their files on request.

B. Student records:

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

- Information which may be sought and recorded when students are referred for 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 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, physical and mental 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
- Academic record – subjects studied, class assignments, examination results as recorded on official School plans.
- Records of significant achievements
- Record of application for support in State examinations, eg. RACE
- Whether the student is repeating the Leaving Certificate
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Garda vetting outcome record (where the student is engaged in work experience organised with or through the school/ETB which requires that they be Garda vetted)
- 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 gather information to inform the enrolment process
- 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, mental and emotional requirements of the student
- to ensure that the student meets the school's admission criteria

- to ensure that students meet the minimum age requirements for their course,
 - to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
 - to furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other Schools etc. in compliance with law and directions issued by government departments
 - to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/ references to third-level educational institutions and/or prospective employers
 - In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the School will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** these files are maintained in both manual and digital format (T-Drive). Manual files are kept in a locked filing cabinet and digital records are maintained with firewall and password protection.

C. Board of Management records:

- (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)
 - 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.
 - Financial Records
- (b) **Purposes:** To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of Board appointments and decisions.
- (c) **Location:** In the Principal's Office and only personnel who are authorised to use the data can access it. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** This file is kept in a manual format in a locked filing cabinet in the Principal's Office. Electronic data is stored on the Principal's computer and maintained with firewall and password protection.

D. Other records:

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive):

Creditors

- (a) **Categories of data:** the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):
- name
 - address
 - contact details
 - PPS number
 - tax details
 - bank details and
 - amount paid.
- (b) **Purposes:** This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** These records are kept in manual format in a locked cabinet in the Principal's Office.

CCTV images/recordings

- (a) **Categories:** CCTV is installed in this school externally to record entry to the school premises. This CCTV system may record images of staff, students and members of the public who visit the premises. CCTV signs are erected on the school premises at entrance gate and at the school door.
- (b) **Purposes:** Safety and security of staff, students and visitors and to safeguard school property and equipment.
- (c) **Location:** Cameras are located externally on walls of the school building. Recording equipment is located in the Staff Office.
- (d) **Security:** Access to images/recordings is restricted to the Principal and I.T. Manager (St Vincent's Hospital). Tapes, DVDs, hard disk recordings are retained for 30 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

Examination results

- (a) **Categories:** The school will hold data comprising examination results in respect of its students. These include class, continuous assessment, mock- examinations results and record of State examinations results, eg. Junior Certificate and Leaving Certificate.
- (b) **Purposes:** The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about progress and to plan for further educational experiences.

Location: In a secure, locked filing cabinet in the Staff 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.

- (c) **Security:** These records are kept in manual files and on computer. Manual files are kept in the relevant area so that school staff have constant access. They are kept in a locked filing cabinet. Some records are maintained on computer and are password protected.

Confidential Records

- (a) The Principal, as Designated Liaison Person for St Joseph's Adolescent School, maintains copies of Confidential Files in the office in a locked cabinet. The Designated Liaison Person (DLP) for SVHF is the Social Worker (St Vincent's Hospital) and she maintains all Confidential Files in her office in the Adolescent Unit.
- (b) These files relate to Child Protection Issues. These are only available on a need-to-know basis to school staff.
- (c) These files contain copies of reports made to HSE and minutes of Child Protection Conferences / Family Welfare Conferences. These are not available to parents. Guardians or parents wishing to access these files will be referred to the authors.
- (d) Personal details relating to individual children and families are made available to HSE Social Workers and Gardai when reporting concerns to these agencies, as required in Child Protection protocols. Where it is safe to do so, the parents are informed that a report is being made and are made aware of the concerns raised, in line with our Child Protection Policy.
- (e) Information contained in these files is confidential and all staff are required to respect this.

Links to other policies and to curriculum delivery

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

The following policies may be among those considered:

- Child Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Enrolment Policy
- Substance Use Policy
- ICT Acceptable Usage 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 requests

Section 3 access request

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

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

Section 4 access request

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

- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- Request must be responded to within 40 days
- 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 St Joseph's Adolescent School, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the school. 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.

Implementation arrangements, roles and responsibilities

In St Joseph's Adolescent School the Board of Management is the Data Controller and the Principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

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

Name	Responsibility
Board of management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities

Administrative personnel: Security, confidentiality
IT personnel: Security, encryption, confidentiality

Ratification & communication

When the Data Protection Policy has been ratified by the Board of Management, it becomes the school's agreed Data Protection Policy. It should then be dated and circulated within the school community. The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on students, staff and others in the school community.

Parents/guardians and students should be informed of the Data Protection Policy from the time of enrolment of the student.

Monitoring the implementation of the policy

The implementation of the policy shall be monitored by the Principal and delegated officers of the Board of Management.

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

Reviewing and evaluating the policy

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

Policy formulated: 25th May 2018

Ratified by Board of Management:

Signature: _____

Chairperson Board of Management

Date: _____

Review Date: _____

