

18

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; students and their parents/guardians; applicants for staff posts within the school; and visitors to the school building. 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 is protected by the school.

**Data Protection Principles**

St Joseph’s Adolescent School is a data controller of personal datarelating to its past, present and future staff, students, parents/guardians and other members of the school community. The school’s policy and procedures, which are in line with Data Protection Principles, are as follows:

* **Obtain and process personal data fairly**:

Student information is gathered with the help of the student, the Multi-Disciplinary Team (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 is 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 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 is only processed in a manner consistent with the purposes for which it was gathered. Information is 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. 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, including two-factor authentication is used to safeguard electronically stored data. Staff should only use devices that have these security features in place.

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

When appropriate staff are obliged to add to staff and student records to keep information updated. Students and parents/guardians will be asked to confirm the accuracy at the point of collection of personal data and to notify the school of any changes in personal data to enable the school to update records accordingly. 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 staff member making that change.

* **Retaining data**:

Student information such as enrolment forms and standardized test results are retained until the student is aged 18 plus 6 years. All other information, such as Individual Education Plans and accident reports are retained indefinitely. Information on staff is retained for the full duration of their tenure at the school plus 6 years. Information on unsuccessful staff applicants is retained for a maximum of eighteen months. Visitor data is retained indefinitely. Covid related data is retained for a month. Specific retention periods are outlined at the end of this policy.

* **Destroying data**:

There is one shredder in the main school office. Data, which is no longer required, will be shredded at the school. Data held electronically will be deleted. A list of all deleted data is held in the school office. Data destruction is verified by the Data Protection Officer, the responsibility of which is with the school Principal.

**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; students and their parents/guardians; applicants for staff posts within the school; and visitors to the school building 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 filingsystem.

**Relevant filing system** means any set of information that, both computerised and hard copy, 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 Controlleri.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 has put in place appropriate governance and management practices to safeguard an 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:

* [Education Act, 1998](http://acts2.oireachtas.ie/zza51y1998.1.html),
* [Education (Welfare) Act, 2000](http://www.oireachtas.ie/documents/bills28/acts/2000/a2200.pdf)
* Education for Persons with Special Educational Needs Act, 2004
* The Freedom of Information Act 1997
* Health Act, 1947
* Children First: National Guidance for the Protection and Welfare of Children (2011)

Other legislation that governs data collection, processing and retention included (but not limited to):

* Terms of Employment (Information) Act, 1994
* Organisation of Working Time Act, 1997
* Protection of Employment Acts, 1977-2007
* Parental Leave Acts, 1998-2006
* Statute of Limitations, 1957
* Safety, Health and Welfare at Work Act, 2005
* Personal Injuries Assessment Board Act, 2003
* Charities Act 2009

**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 Principal 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 - collection, processing, storage and destruction.**

The *Personal Data* records held by the school is listed in the data register (appendix 1) which is updated as required. The data register outlines the basis for the collection of this data, how it is processed, for what purpose and how this data is stored and subsequently destroyed.

**Processing in line with data subject’s rights**

Data is processed in line with the data subject’s 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 Act, 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 1 month.

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 1 month
	+ No fee can be applied
	+ 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.

**Data Breach:**

If a data breach occurs, the following procedures will be followed in accordance to the General Data Protection Regulations.

* All breach notifications must be notified to the Data Protection Commission within 72 hours of becoming aware of the breach using the Breach Notification Form. This notification must be made whether or not the details are available. An update to the initial report can be submitted once all the relevant details have been collected.
* Where the breach results in a high risk to a data subject, they must also be notified. If their risk is determined not to require notifying the subject, St. Joseph’s Adolescent School will still retain their own internal records.
* Breach notifications to the Data Protection Commission can be done by online using the breach notification form: www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification
* Personal information of the affected individuals should not be included in the email.
* The breach requires a self-declared risk notification:
	+ **Low Risk:** The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal.
	+ **Medium Risk:** The breach may have an impact on individuals, but the impact is unlikely to be substantial.
	+ **High Risk:** The breach may have a considerable impact on affected individuals.
	+ **Severe Risk:** The breach may have a critical, extensive, or dangerous impact on affected individuals

**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 and Data Protection Officer

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 as the Data Protection Officer.

At least one report annually 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), 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 updated: 27th April 2022Ratified by Board of Management:Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Chairperson Board of ManagementDate: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Review Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  |

Appendix 1-Data Privacy Statements

**Privacy Policy - Recruitment**

As a personal data controller, St Joseph’s Adolescent School respects your privacy and is committed to protecting your personal data. This means that we are responsible for deciding how we hold and use personal data about you. This notice sets out how and why your personal data will be used, namely for the purposes of recruitment and how long it will be retained for.

**Data Protection Principles**

We will comply with data protection law and principles, which means that your data will be:

* Used lawfully, fairly and in a transparent way.
* Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
* Relevant to the purposes we have told you about and limited only to those purposes.
* Accurate and kept up to date.
* Maintained only for as long as necessary for the purposes we have told you about, i.e. in relation to the recruitment exercise.
* Kept securely and protected against unauthorised or unlawful processing and against loss or destruction using appropriate technical and organisational measures.

**What data do we hold about you?**

In connection with your application, we will collect, use and store the following categories of personal data about you:

* The data you have provided to us in your curriculum vitae (CV) and the personal data contained in your covering letter.
* The data you have provided as part of the application process, including name, title, address, telephone number, personal email address, date of birth, employment history, qualifications, professional memberships, educational achievements, diplomas, transcripts, languages, computer skills, and any data you provide us during interviews at our premises.
* Any personal data provided to us about you by your referees [if applicable].

**HOW IS YOUR PERSONAL DATA COLLECTED?**

We collect personal data about candidates from the following sources:

* You, the candidate.
* Your named referees, from whom we collect the following categories of data: full name, periods of previous employment, performance during previous employment.

**HOW WE WILL USE DATA ABOUT YOU**

We will use the personal data we collect about you to:

* Assess your skills, qualifications, and suitability for the role.
* Carry out background and reference checks, where applicable.
* Communicate with you about the recruitment process.
* Keep records related to our hiring processes.
* Comply with legal or regulatory requirements.

It is in our legitimate interests to decide whether to appoint you to the role since it would be beneficial to the school to appoint a suitable candidate to that role.

We also need to process your personal data to decide whether to enter into a contract with you.

Having received your CV and covering letter, we will then process that data to decide whether you meet the requirements to be shortlisted for the role. If you do, we will decide whether your application is suitable to invite you for an interview. If we decide to call you for an interview, we will use the data you provide to us at the interview to decide whether to offer you the role. If we decide to offer you the role, we may then take up references and/or any other check before confirming your appointment.

**If you fail to provide personal data**

If you fail to provide personal data when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we may not be able to process your application further. For example, if we require references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

**HOW WE USE PARTICULARLY SENSITIVE PERSONAL DATA**

We will use your sensitive personal data only in so far as we are permitted by Law to do so :

In the event that you have a disability, we will only use data about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during the interview.

**DATA SHARING**

We will only share your personal data with the following third parties for the purposes of processing your application: Interview Board, Board of Management and the CDETB (where they are funding the position).

**DATA SECURITY**

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

**DATA RETENTION**

If successful, we will retain your information for the duration of your employment plus 7 years. If you are unsuccessful, we will retain your personal data for a period of 18 months from close of competition plus 6 months in case the Equality Tribunal needs to inform school that a claim is being made. We retain your personal data for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have recruited in a fair and transparent way. We further retain such personal data in case a similar role becomes vacant for which you will be a suitable candidate. After this period, we will securely destroy your personal data in accordance with our data retention policy.

**RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION**

**Your rights in connection with personal data**

Under certain circumstances, by law you have the right to:

* **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
* **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data corrected.
* **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
* **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.
* **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
* **Request the transfer** of your personal data to another party.

If you want to review, verify or correct your personal data, you can do so by logging into the online system. If you wish to request erasure of your personal data or object to the processing of your personal data, please send an email to principal@svhf.ie.

**ADDRESS DATA PROTECTION QUERIES**

We have appointed a Data Protection Officer [ DPO, Principal-Michael O’Brien] to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal data, please contact the DPO at 01-8842441 or at principal@svhf.ie.

Appendix 2

Click the link below for the most recently updated Data Register

[Data *Register* SJAS](https://stjosephsadolescentschool-my.sharepoint.com/%3Ax%3A/r/personal/michaelobrien_stjosephsadolescentschool_onmicrosoft_com/_layouts/15/Doc.aspx?sourcedoc=%7BABD248DA-0DC7-4382-8C7C-56B4907F02D4%7D&file=Data%20Register%202022%20(1).xlsx&action=default&mobileredirect=true)