

# St. Joseph's National School



## Data Protection Policy

### Introduction:

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

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

### Rationale:

- A policy on data protection and record keeping is necessary to ensure that the school has proper procedures in place in relation to accountability and transparency;
- It is good practice to record pupil progress so as to identify learning needs;

### Relationship to School Ethos:

We promote openness and co-operation among staff, parents, management and pupils as a means towards providing the caring environment through which a child can develop and grow to full potential.

### Aims/Objectives:

- To ensure the school complies with legislative requirements;
- To clarify the types of records maintained and the procedures relating to making them available to the relevant bodies;
- To put in place a proper recording and reporting framework on the educational progress of pupils;
- To establish clear guidelines on making these records available to parents (and pupils over 18);
- To stipulate the length of time records and reports will be retained;

### **Data Protection Guidelines:**

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 and until he/she turns 21 years of age. 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.

The Principal assumes the function of *data controller* and supervises the application of the Data Protection Act within the school. The data under the control of the Principal comes under the following headings.

#### **Purpose:**

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.

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

#### **Definition of terms:**

**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, St. Joseph's N.S.

**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).

#### **Personal Data:**

This data relates to personal details of the students such as name, address, date of birth, gender, home telephone and mobile contact details, ethnic origin, nationality, religious belief, medical details, dietary information, (PPSN in the case of students with special educational needs).

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

#### **Staff records:**

- (a) **Categories of staff data:** As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:
- Name, address and contact details, PPS number
  - 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.)
  - Garda Vetting
  - Medmark
  - 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:** 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:** Filing cabinet in Principal's office and Aladdin.

#### **Student records:**

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

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
  - name, address and contact details, PPS number
  - date and place of birth
  - names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
  - religious belief
  - racial or ethnic origin
  - membership of the Traveller community, where relevant
  - whether they (or their parents) are medical card holders
  - whether English is the student's first language and/or whether the student requires English language support
  - any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply

- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student)
- Psychological, psychiatric and/or medical assessments
- Attendance records
- Photographs and recorded images of students (including at school events and noting achievements). See the template “Guidance on Taking and Using Images of Children in Schools”
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under 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 “Guidance for Taking and Using Images of Pupils in Schools” (see template)
- 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
- (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:** Filing cabinet in Principal's office and Aladdin.

#### **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 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.
- (c) **Location:** The Principal's Office. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** Filing cabinet in Principal's office and Aladdin.

#### **CCTV images/recordings:**

- (a) **Categories:** CCTV is installed in some schools, externally i.e. perimeter walls/fencing and internally as detailed in the CCTV Policy. These CCTV systems may record images of staff, students and members of the public who visit the premises.
- (b) **Purposes:** Safety and security of staff, students and visitors and to safeguard school property and equipment.
- (c) **Location:** Cameras are located externally and internally. Recording equipment is located in the store room near the office.



- (d) **Security:** Access to images/recordings is restricted to the principal & deputy principal of the school. Tapes, DVDs, hard disk recordings are retained for 28 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, mid-term, annual, continuous assessment examinations results.
- (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 subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

**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.

- (c) **Security:** Filing cabinet in Principal's office and Aladdin.

#### **Data Access Requests:**

The following will have access where relevant and appropriate to the data listed above where pupils are identified by name:

- Parents/Guardians
- Past Pupils over 18
- Health Service Executive staff
- National Educational Psychological Service
- National Education Welfare Board
- Occupational Therapists or Speech Therapists working with pupils
- Designated School Personnel
- Department of Education and Skills (where necessary)
- First and Second level schools (once it has been confirmed by that school that the child has been enrolled)
- St. Joseph's N.S. Board of Management

With the exception of child protection-related data which is governed by "Children's' First Guidelines and Procedures 2011", data on attendance, (governed by NEWB) and data regarding achievements in literacy and numeracy, (governed by National Strategy for literacy and numeracy), parental authorisation must be provided by parents in the event of data

being transferred to outside agencies. Outside agencies requesting access to records must do so in writing. Parents/Guardians of current pupils can make such a request either by phone or in writing. Past pupils and parents of past pupils seeking data must do so in writing.

A standardised school report form, provided by the National Council for Curriculum and Assessment are issued by post in June to all parents along with results of standardised testing of pupils from 1<sup>st</sup> to 6<sup>th</sup> classes.

### 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) Appendix 1
- 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.

### Phone requests

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.

### **Implementation:**

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

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

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

### **Storage:**

Records are kept until the pupil reaches 21 years of age. Standardised tests booklets are shredded but the percentiles are kept on record until past pupils reach adulthood, (21 years of age). Scores are added to Aladdin from 2016.

- As children pass to second level, their records are stored in the strong room (labelled with the school year in which they completed 6<sup>th</sup> class) until the pupil reaches 21 years of age.
- All completed school roll books and school registers are stored in the strong room indefinitely. Access to these stored files is restricted to authorised personnel only.

### **Success Criteria:**

- Compliance with Data Protection Act and Statute of Limitations Act.
- Reasonably easy access to records
- Manageable storage of records.

### **Roles and Responsibilities:**

The school staff, under the direction of the Principal, will implement and monitor this policy. Individual teachers will design, administer and record in-class testing. The Principal and Deputy Principal will ensure records are maintained and stored.

### **Roles and Responsibility.**

Teaching Staff

Board of Management

**Implementation Data:** April 2017

**Review Date:** June 2020

Ratified by the Board of Management

Signed \_\_\_\_\_ Chairperson, Board of Management

Signed \_\_\_\_\_ Principal

Date \_\_\_\_\_

## Appendix 1

### Exceptions to the Right of Access

Individuals have a strong right of access to see their personal data. However, section 5 of the Data Protection Acts provides that individuals do not have a right to see information relating to them where any of the following circumstances apply.

1. If the information is kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing / collecting any taxes or duties: but only in cases where allowing the right of access would be likely to impede any such activities  
Comment: It would obviously be unacceptable to allow a criminal suspect to see all of the information kept about him by An Garda Síochána, where this would be likely to impede the effectiveness of the criminal investigation. On the other hand, however, if allowing an individual access to personal information about him or her would not be likely to impede an investigation, then the access request would have to be complied with. (see [case study 2/04](#))
2. If granting the right of access would be likely to impair the security or the maintenance of good order in a prison or other place of detention
3. If the information is kept for certain anti-fraud functions: but only in cases where allowing the right of access would be likely to impede any such functions
4. If granting the right of access would be likely to harm the international relations of the State
5. If the information concerns an estimate of damages or compensation in respect of a claim against the organisation, where granting the right of access would be likely to harm the interests of the organisation
6. If the information would be subject to legal professional privilege in court
7. If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved
8. If the information is back-up data.  
Comment: It would be unreasonable to expect an organisation to retrieve back-up copies of its personal information in responding to an access request. However, it should be noted that back-up data is not necessarily the same as old or archived data. Such archive data is subject to an individual's right of access in the normal way.

### Restrictions on access to medical data and social work data.

[The Data Protection \(Access Modification\) \(Health\) Regulations, 1989 \(S.I. No. 82 of 1989\)](#) provide that health data relating to an individual should not be made available to the individual, in response to an access request, if that would be likely to cause serious harm to the physical or mental health of the data subject. A person who is not a health professional should not disclose health data to an individual without first consulting the individual's own doctor, or some other suitably qualified health professional. Similar provisions apply in respect of social work data. The Data Protection (Access Modification) (Social Work) Regulations, 1989 (S.I. No. 83 of 1989) provide that social work data relating to an individual should not be made available to the individual in response to an access request, if that would be likely to cause serious harm to the physical or mental health

or emotional condition of the data subject. The regulations apply to social work carried on by Ministers, local authorities, health boards, or any voluntary or other body that receives public funding for this work.

### **Information about Other Individuals**

Section 4(4) of the Data Protection Act makes special provision for dealing with the personal data of another individual. A data controller is not obliged to comply with an access request if that would result in disclosing data about another individual, unless that other individual has consented to the disclosure. However, the data controller is obliged to disclose so much of the information as can be supplied without identifying the other individual, e.g. by omitting names or other identifying particulars.

### **Expressions of opinion**

Where personal data consists of an expression of opinion about the data subject by another person, the data subject has a right to access that opinion except if that opinion was given in confidence. If the opinion was not given in confidence then the possible identification of the individual who gave it does not exempt it from access.

### **Examinations Data**

Section 4(6) of the Data Protection Act makes special provision for responding to an access request about the results of an examination. "Examination" in this context means any test of knowledge, skill, ability etc., and is therefore not confined to official State examinations. Medical examinations are not covered, though. These special rules

- (a) increase the time limit for responding to an access request from 40 days to 60 days, and
- (b) deem an access request to be made at the date of the first publication of the examination results or at the date of the request, whichever is the later.

### **Disproportionate effort**

Section 4(9) provides that the obligation on a data controller to comply with an access request, should normally be met by supplying a copy in permanent form, unless the supply of such a copy is not possible or would involve disproportionate effort.

### **Repeated Access Requests**

If a data controller has complied with an access request he does not have to comply with an identical or similar request unless a reasonable interval has elapsed