
St. Patrick's Loreto Primary School

Data Protection Policy

Table of Contents

1. Introduction	1
2. Purpose and Scope	2
3. Processing Principles	2
4. Lawful Basis for Processing Personal Data	3
5. Processing Activities undertaken by the School	4
6. Recipients	5
7. Personal Data Breaches	6
8. Data Subject Rights	7
9. Managing Data Requests	8
Appendices	12
1. Data Access Request Form	
2. Records Retention Schedule	
3. Reference Sites	

1 Introduction

The characteristic spirit of St. Patrick's Loreto Primary School has at its core a desire to promote and protect the dignity of every member of its community, students, staff and parents. This policy applies to all school staff, the Board of Management, parents/ guardians, pupils (including prospective pupils) and their parents/ guardians and applicants for positions within the school.

The Board of Management of St. Patrick's Loreto Primary School is committed to the principles of responsible data protection as outlined in relevant legislation and, to this end, it will:

- Obtain and fairly process personal data
- Keep data for one or more specified lawful purposes
- Process only data in ways compatible with the purposes for which it was given initially

- Securely store personal data
- Ensure that personal data is accurate and up-to-date
- Ensure that only relevant data is sought and stored
- Retain data no longer than is necessary for the specified purpose or purposes for which it was given
- Comply with request for data, as outlined in relevant legislation

2 Purpose and Scope

The purpose of this Data Protection Policy is to support the school in meeting its responsibilities with regard to the processing of personal data. These responsibilities arise as statutory obligations under the relevant data protection legislation. They also stem from our desire to process all personal data in an ethical manner which respects and protects the fundamental rights and freedoms of natural persons.

This policy aims to help transparency by identifying how the school expects personal data to be treated (or “processed”). It helps to clarify what data is collected, why it is collected, for how long it will be stored and with whom it will be shared.

The Irish *Data Protection Act (2018)* and the European *General Data Protection Regulation (2016)* are the primary legislative sources.¹ As such they impose statutory responsibilities on the school as well as providing a number of fundamental rights (for students, parents/guardians and staff and others) in relation to personal data.

The school recognises the seriousness of its data processing obligations and has implemented a set of practices to safeguard personal data. Relevant policies and procedures apply to all school staff, boards of management, trustees, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school).

Any amendments to this Data Protection Policy will be communicated through the school website and other appropriate channels, including direct communication with data subjects where this is appropriate. We will endeavour to notify you if at any time we propose to use Personal Data in a manner that is significantly different to that stated in our Policy, or, was otherwise communicated to you at the time that it was collected.

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. Formally, the statutory responsibility of Controller is assigned to the Board of Management. The Principal is assigned the role of co-ordinating the implementation of this Policy and for ensuring that all staff who handle or have access to Personal Data are familiar with their responsibilities.

Name	Responsibility
Board of Management	Data Controller
Principal	Implementation of Policy
All Staff	Adherence to the Data Processing Principles
Entire School Community	Awareness and Respect for all Personal Data

3 Processing Principles

Processing is the term used to describe any task that is carried out with personal data e.g. collection, recording, structuring, alteration, retrieval, consultation, erasure as well as disclosure by transmission, dissemination or otherwise making available. Processing can include any activity that might relate to personal data under the control

¹ The school is also cognisant of other legislation which relates to the processing of personal data, whether in manual or in electronic form. For example, the 2011 e-Privacy Regulations (S.I. No. 336 of 2011) provide statutory guidance with regard to certain data processing operations (e.g. direct marketing, cookie notifications on school website etc.).

of the school, including the storage of personal data, regardless of whether the records are processed by automated or manual means.

There are a number of fundamental principles, set out in the data protection legislation, that legally govern our treatment of personal data. As an integral part of its day to day operations, the school will ensure that all data processing is carried out in accordance with these processing principles.

These principles, set out under GDPR, establish a statutory requirement that personal data must be:

- (i) processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**);
- (ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (**purpose limitation**);
- (iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**);
- (iv) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**accuracy**);
- (v) kept for no longer than is necessary for the purposes for which the personal data are processed²; (**storage limitation**);
- (vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

GDPR also establishes **Accountability** as a core data processing principle. This places a statutory responsibility on the school, as Data Controller, to be able to demonstrate compliance with the other principles i.e. the 6 data processing principles set out in the previous paragraph.

4. Lawful Basis for Processing Personal Data

Whenever the school is processing personal data, all of the principles listed in the previous section(s), must be obeyed. In addition, at least one of the following bases (GDPR Article 6) must apply if the processing is to be lawful,

- (i) compliance with a legal obligation
- (ii) necessity in the public interest
- (iii) legitimate interests of the controller
- (iv) contract
- (v) consent
- (vi) vital interests of the data subject.

When processing **special category personal data**, the school will ensure that it has additionally identified an appropriate lawful basis under GDPR Article 9.³ Special categories of personal data are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

² Data may be stored for longer periods if being processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (subject to appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject).

³ GDPR Article 9 sets out the lawful bases that apply to the processing of special categories of personal data.

5. Processing Activities Undertaken by the School

Record of Processing Activities This policy sets out the purposes for which the school collects and uses personal data for each of the various categories of data held (student, staff, parent, etc).

All data will be retained as outlined in the Retention Schedule below (Appendix 2).

The school computer system falls under The Schools Broadband Programme, which provides an integrated set of services to schools which includes broadband connectivity, hosted services including content filtering, security services including anti-virus control and a centralised firewall. In addition, password protected documents are stored under Microsoft platform security. Microsoft accounts are set up using individual, secure passwords for each account.

Student Records The purposes for processing student personal data include the following: ⁴

- (i) to provide information prior to application/enrolment;
- (ii) to determine whether an applicant satisfies the school's admission criteria;
- (iii) to comprehend the educational, social, physical and emotional needs of the student;
- (iv) to deliver an education appropriate to the needs of the student;
- (v) to ensure that any student seeking an exemption from Irish meets the criteria;
- (vi) to ensure that students benefit from relevant additional educational or financial supports;
- (vii) to contact parents/guardians in case of emergency or in the case of school closure;
- (viii) to monitor progress and to provide a sound basis for advising students and parents/guardians;
- (ix) to inform parents/guardians of their child's educational progress etc.;
- (x) to communicate information about, and record participation in, school events etc.;
- (xi) to compile yearbooks, establish a school website, and to keep a record of the history of the school;
- (xii) to comply with legislative or administrative requirements;
- (xiii) to furnish documentation/ information about the student to the Department of Education, the National Council for Special Education, TUSLA, and others in compliance with law and directions issued by government departments.

Pupil data is kept both in manual form in a locked filing cabinet, and on the school computer system and Databiz.

The Board of Management has a service agreement with Databiz which confirms that they adhere to GDPR principles when processing pupil data. Data held on Databiz is protected by passwords known to the Principal and Chairperson to the Board of Management and other school personnel who are authorised by the Chairperson or Principal to use the data can access it.

Particularly sensitive information (e.g. TUSLA referrals, court orders etc.) should only be stored in the Principal's office in a locked filing cabinet. Teacher and SNA notes should be stored within the classroom.

Parent/Guardian Records The school does not keep personal files for parents or guardians. However, information about, or correspondence with, parents may be held in the files for each student. This information shall be treated in the same way as any other information in the student file.

Staff Records As well as records for existing members of staff (and former members of staff), records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. The purposes for which staff personal data is processed include the following:

- (i) the management and administration of school business (now and in the future);

⁴ Appendix 5 sets out the type of personal data being processed by the school and the purposes for which this data is being processed. This list is likely to be subject to revision from time to time. For example, changes in curriculum or legislation may require adjustments in the personal data processing.

- (ii) 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);
- (iii) to facilitate pension payments in the future;
- (iv) human resources management;
- (v) recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.;
- (vi) 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*);
- (vii) to enable the school to comply with requirements set down by the Department of Education, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies;
- (viii) and for compliance with legislation relevant to the school.

Staff data is kept both in manual form, within a locked filing cabinet in the Principal's office, and on the school computer system and Databiz. The Board of Management has a service agreement with Databiz which confirms that they adhere to GDPR principles when processing data. Data held on school computers and Databiz is protected by passwords known to the Principal and Chairperson to the Board of Management. Only personnel who are authorised by the Chairperson of Principal to use the data can access it.

Board of Management Records Board of Management records are kept in accordance with the Education Act 1998 and other applicable legislation. Minutes of Board of Management meetings record attendance, items discussed and decisions taken. Board of Management business is considered confidential to the members of the Board and is kept within a locked filed cabinet in the Principal's office, and/or locked room (e.g. Archive Room) and on the school's computer system. Data held on school computers is protected by passwords known to the Principal and Chairperson to the Board of Management.

Financial Records This information is required for routine management and administration of the school's financial affairs, including the payment of fees, invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners. These records are kept in the school office and/or on the password-protected Office computer account.

CCTV Records The school processes personal data in the form of recorded CCTV images. We use CCTV for the following purposes:

- (i) to secure and protect the school's premises and assets;
- (ii) to deter crime and anti-social behaviour;
- (iii) to assist in the investigation, detection, and prosecution of offences;
- (iv) to monitor areas in which cash and/or goods are handled;
- (v) to deter bullying and/or harassment;
- (vi) to maintain good order and ensure the school's Code of Behaviour is respected;
- (vii) to provide a safe environment for all staff and students;
- (viii) for the taking and defence of litigation;
- (ix) for verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and where the recordings may be capable of resolving that dispute.

CCTV records are kept for a maximum of twenty-eight days, except if required for an investigation. Only the Chairperson of the Board of Management, Principal, Deputy Principal (in the absence of the Principal), school caretaker and members of An Garda Siochana may view CCTV recordings.

If a person wishes to access CCTV recordings, a data access request form (Appendix 1) must be completed. Persons are not entitled to any CCTV footage that identifies third parties. If requested CCTV footage requires third parties to be redacted, and depending on the cost associated with pixelating and/ or blurring third parties, the Board of

Management may refuse the data access request form if it is an excessive cost to bear for the Board. Further details are available in Section 9 of this policy.

6. Recipients

Recipients These are defined as organisations and individuals to whom the school transfers or discloses personal data. Recipients may be data controllers, joint controllers or processors. A list of the categories of recipients used by the school is provided in the appendices (Appendix 3). This list may be subject to change from time to time.

Data Sharing Guidelines

- (i) From time to time the school may disclose Personal Data to third parties, or allow third parties to access specific Personal data under its control. An example could arise should Gardai submit a valid request under Section 41(b) of the Irish Data Protection Act which allows for *processing necessary and proportionate for the purposes of preventing, detecting, investigating or prosecuting criminal offences*.
- (ii) In all circumstances where personal data is shared with others, the school will ensure that there is an appropriate lawful basis in place (GDPR Articles 6, 9 as appropriate). We will not share information with anyone without consent unless another lawful basis allows us to do so.
- (iii) Most data transfer to other bodies arises as a consequence of legal obligations that are on the school, and the majority of the data recipients are Controllers in their own right, for example, the Department of Education. As such their actions will be governed by national and European data protection legislation as well their own organisational policies.⁵
- (iv) Some of the school's operations require support from specialist service providers. For example, the school may use remote IT back-up and restore services to maintain data security and integrity. In cases such as these, where we use specialist data processors, we will ensure that the appropriate security guarantees have been provided and that there is a signed processing agreement in place.

7. Personal Data Breaches

Definition of a Personal Data Breach A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Consequences of a Data Breach

- i. A breach can have a significant adverse effect on individuals, which can result in physical, material or non-material damage. This can include discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality etc. Children, because of their age, may be particularly impacted.
- ii. In addition to any detrimental impact on individual data subjects, a data breach can also cause serious damage to the school. This can include reputational damage as well as exposing the school to other serious consequences, including civil litigation.
- iii. It should be noted the consequences of a data breach could include disciplinary action, criminal prosecution and financial penalties or damages for the school and participating individuals.⁶

⁵ The Data Protection Policy of the Department of Education can be viewed on its website (www.education.ie).

⁶ The Data Protection Act 2018 established a number of offences whereby breaches of the Act can result in fines and/or imprisonment.

Responding to a Data Breach

- iv. The school will always act to prioritise and protect the rights of those individuals whose personal data is affected.
- v. As soon as the school becomes aware that an incident has occurred, measures will be taken to assess and address the breach appropriately, including actions to mitigate any possible adverse effects.
- vi. Where the school believes that there is a risk to the affected individuals, the school will (within 72 hours of becoming aware of the incident) submit a report to the Data Protection Commission.
- vii. Where a breach is likely to result in a high risk to the affected individuals, the school will inform those individuals without undue delay.
- viii. The school will maintain a data breach log.

Data Breach Protocol

- i. If a data breach occurs, inform the Principal immediately.
- ii. The Principal* should take immediate steps to retrieve and/ or delete the data permanently.
- iii. Written confirmation should be sought from all persons who received the data to confirm the following:
 1. That the data concerned has been deleted (e.g. email, contact details, attachment, document etc.);
 2. That the data has not been further distributed or transferred the email and attachment;
 3. That the information in the data has not and will not be used for any purpose;
 4. That (if necessary) this confirmation can be shared with a third party (e.g. data subject, Data Protection Commission etc.), redacting personal details where possible
- iv. In line with the legislation, and within 72 hours and without undue delay, the Principal shall inform the Chairperson of the Board of Management, the school insurer and the Data Protection Commission, where appropriate.
- v. In line with the legislation, and within 72 hours and without undue delay, the Principal shall inform the affected persons, where appropriate. A written letter may be sent to the affected persons outlining what happened, what information was shared and what steps are being taken to rectify the situation. The Principal will offer to meet with the affected persons.
- vi. The Principal shall review current data sharing protocols and systems to mitigate against future data breaches.
- vii. The data breach will be added to the Data Breach Log.
- viii. The Principal will keep a log of actions of all steps taken.
- ix. The school will cooperate fully with any investigation, where appropriate.

**If the Principal is not available, the Deputy Principal should initiate the Data Breach Protocol. If the Deputy Principal is not available, the Assistant Principal (in order of seniority) will initiate it.*

Procedure for Sharing Password-Protected Correspondence

- i. All password-protected correspondence received to the school office and/or teacher's emails should be forwarded to the Principal (or Deputy Principal in their absence)
- ii. The Principal can advise on appropriate next steps.
- iii. If the Principal decides that an encrypted document can be shared, ensure the password is shared in a separate email. Never put a password and an encrypted document in the same email.
- iv. When handling sensitive data, and where possible, children's initials, not full names, should be used in the body of email correspondence.
- v. If a data breach occurs, inform the Principal immediately. The Data Breach Protocol will be initiated (See above).

8. Data Subject Rights

Your Rights Personal Data will be processed by the school in a manner that is respectful of the rights of data subjects. Under GDPR these include⁷

- (i) the right to information
- (ii) the right of access
- (iii) the right to rectification
- (iv) the right to erasure (“right to be forgotten”)
- (v) the right to restrict processing
- (vi) the right to data portability
- (vii) the right to object
- (viii) the right not to be subject to automated decision making
- (ix) the right to withdraw consent
- (x) the right to complain.

Right to be Informed You are entitled to information about how your personal data will be processed. We address this right primarily through the publication of this Data Protection Policy. We also publish additional privacy notices/statements which we provide at specific data collection times, for example, our Website Data Privacy Statement is available to all users of our website. Should you seek further clarification, or information that is not explicit in our Policy or Privacy Statements, then you are requested to forward your query to the school.

Right of Access You are entitled to see any information we hold about you. The school will, on receipt of a request from a data subject, confirm whether or not their personal data is being processed. In addition, a data subject can request a copy of their personal data. The school in responding to a right of access must ensure that it does not adversely affect the rights of others.

Right to rectification If you believe that the school holds inaccurate information about you, you can request that we correct that information. The personal record may be supplemented with additional material where it is adjudged to be incomplete.

Right to be forgotten Data subjects can ask the school to erase their personal data. The school will act on such a request providing that there is no compelling purpose or legal basis necessitating retention of the personal data concerned.

Right to restrict processing Data subjects have the right to seek a restriction on the processing of their data. This restriction (in effect requiring the controller to place a “hold” on processing) gives an individual an alternative to seeking erasure of their data. It may also be applicable in other circumstances such as where, for example, the accuracy of data is being contested.

Right to data portability This right facilitates the transfer of personal data directly from one controller to another. It can only be invoked in specific circumstances, for example, when processing is automated and based on consent or contract.

Right to object Data subjects have the right to object when processing is based on the school’s legitimate interests or relates to a task carried out in the public interest (e.g. the processing of CCTV data may rely on the school’s legitimate interest in maintaining a safe and secure school building). The school must demonstrate compelling legitimate grounds if such processing is to continue.

Right not to be subject to automated decision making This right applies in specific circumstances (as set out in GDPR Article 22).

⁷ For further information on your rights see www.GDPRandYOU.ie.

Right to withdraw consent In cases where the school is relying on consent to process your data, you have the right to withdraw this at any time, and if you exercise this right, we will stop the relevant processing.

Limitations on Rights While the school will always facilitate the exercise of your rights, it is recognised that they are not unconditional: the school may need to give consideration to other obligations.⁸

Right to Complain

- i. If you are concerned about how your personal data is being processed, then please address these concerns in the first instance to the Principal who is responsible for operational oversight of this policy.⁹
- ii. A matter that is still unresolved may then be referred to the school's Data Controller (i.e., the Board of Management) by writing to the Chairperson c/o school.
- iii. Should you feel dissatisfied with how we have addressed a complaint or concern that you have raised, you have the right, as data **subject**, to bring the matter to the attention of the Irish Data Protection Commission.

Telephone	+353 57 8684800 +353 (0)761 104 800
Lo Call Number	1890 252 231
Fax	+353 57 868 4757
E-mail	info@dataprotection.ie
Post	Data Protection Commission Canal House, Station Road Portarlinton, Co. Laois R32 AP23
Website	www.dataprotection.ie

⁸ See GDPR Articles 12-23 for a full explanation of subject rights and their application.

⁹ Parents/Guardians may also, where applicable, have the option of invoking the school's formal complaints procedure (available from school).

9. MANAGING DATA REQUESTS

1. Responding to rights requests

- (i) The school will log the date of receipt and subsequent steps taken in response to any valid request. This may include asking the data subject to complete an *Access Request Form* (Appendix 1) in order to facilitate efficient processing of the request. There is no charge for this process.¹⁰
- (ii) Under its obligation in relation to the Children First Act (2015), the school will cooperate fully with data access requests from TUSLA.
- (iii) Having established the lawful reason for the sharing of data, the school will cooperate with data access requests from An Garda Síochána, HSE and Department of Social Protection. The school reserves the right to request a written letter to confirm the basis for the lawful reason to access requested data.
- (iv) The school is obliged to confirm the identity of anyone making a rights request and, where there is any doubt on the issue of identification, will request official proof of identity (e.g. photographic identification such as a passport or driver's licence).¹¹
- (v) If requests are manifestly unfounded or excessive¹², in particular because of their repetitive character, the school may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or refuse to act on the request.
- (vi) The school will need to confirm that sufficient information to locate the data requested has been supplied (particularly if CCTV footage/images are to be searched¹³). Where appropriate the school may contact the data subject if further details are needed.
- (vii) In responding to rights requests (e.g. data access requests) the school will ensure that all relevant manual¹⁴ and automated systems (computers etc.) are checked.
- (viii) The school will be conscious of the need to respond without undue delay and within the advised timeframes. A response will be made within one month of receipt of any request.¹⁵
- (ix) The school must be conscious of the restrictions that apply to rights requests.¹⁶ Where unsure as to what information to disclose, the school reserves the right to seek legal advice.¹⁷
- (x) Where a request is not being fulfilled, the data subject will be informed as to the reasons and the mechanism for lodging a complaint, including contact details for the Data Protection Commission.
- (xi) Where action has been taken by the school with regard to rectification, erasure or restriction of processing, the school will ensure that relevant recipients (i.e. those to whom the personal data has been disclosed) are appropriately informed.

¹⁰ The school may charge a reasonable fee for any further copies requested by the data subject, or where access requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information. Where a subsequent or similar access request is made after the first request has been complied with, the school has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.

¹¹ Where a subject access request is made via a third party (e.g. a solicitor) the school will need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement.

¹² In such circumstances, the school must be able to demonstrate the manifestly unfounded or excessive character of a request.

¹³ The school will always endeavour to respond to any access request within the stipulated time period. However a timely response can be greatly facilitated by provided (in writing to the school) all necessary information such as date, time and location of any recording.

¹⁴ Non-automated personal data that is held within a filing system or intended to form part of a filing system (GDPR Article 2).

¹⁵ That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The school must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

¹⁶ See for example GDPR Article 23 and Irish Data Protection Act 2018 S.56, S.60, S.61.

¹⁷ Decisions around responding to data access requests will need to give due regard to rights and responsibilities that derive from other legislation, not least Article 42A of the Irish Constitution which recognises and affirms the natural and imprescriptible rights of all children. Examples of other factors that might need to be considered include: any court orders relating to parental access or responsibility that may apply; any duty of confidence owed to the child or young person; any consequences of allowing those with parental responsibility access to the child's or young person's information (particularly important if there have been allegations of abuse or ill treatment); any detriment to the child or young person if individuals with parental responsibility cannot access this information; and any views the child or young person has on whether their parents should have access to information about them.

2. Format of Information supplied in fulfilling a request

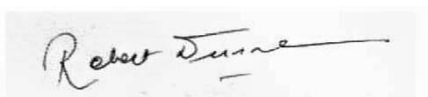
- (i) The information will be provided in writing, or by other means, including where appropriate, by electronic means. (When requested by a data subject the information access may be provided in alternative means e.g. orally.)
- (ii) The school will endeavour to ensure that information is provided in an intelligible and easily accessible format.

10. Communication, Monitoring and Review

This policy was ratified by St. Patrick's Loreto Primary School's Board of Management on 19th October 2023.

This policy will be communicated to staff and the school community, as appropriate. It will be reviewed initially every three years, unless there is a compelling reason to review it earlier.

Signed:



Date: 19th October 2023

Chairperson, Board of Management

APPENDIX 1

ST. PATRICK'S LORETO PRIMARY SCHOOL

DATA ACCESS REQUEST FORM

Request for a copy of Personal Data under the Data Protection Acts 1988 to 2018

Important: Proof of Identity must accompany this Access Request Form (eg. official/State photographic identity document such as driver's licence, passport).

Full Name:	
Maiden Name <i>(if name used during your school duration)</i>	
Address:	
Contact number *	Email addresses *

* We may need to contact you to discuss your access request

Please tick the box which applies to you:

Parent/ Guardian of current Pupil <input type="checkbox"/>	Former Pupil <input type="checkbox"/>	Current Staff Member <input type="checkbox"/>	Former Staff Member: <input type="checkbox"/>
--	---	---	---

Name of Pupil:		Date of Birth of Pupil:	
Insert Year of leaving:		Insert Years From/To:	

Data Access Request:

I, [name] wish to make an Access Request for a copy of personal data that St. Patrick's Loreto Primary School holds about me/my child. I am making this access request under Data Protection Acts 2013 to 2018

To help us to locate your personal data, please provide details below, which will assist us to meet your requirements e.g. description of the category of data you seek

Any other information relevant to your access request (e.g. if requesting images/recordings made by CCTV, please state the date, time and location of the images/recordings as otherwise it may be very difficult or impossible for the school to locate the data)

This **Access Request** must be accompanied with a copy of photographic identification e.g., passport or driver's licence. I declare that all the details I have given in this form are true and complete to the best of my knowledge.

Signature of Applicant Date:

Please return this form to the relevant address:

To the Chairperson of Board of Management, St. Patrick's Loreto Primary School, Vevay Road, Bray. Co. Wicklow.

APPENDIX 2 RECORDS RETENTION SCHEDULE

Schools 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 anonymised to remove any personal data. Anonymisation must be irrevocable; removing names and addresses may not necessarily be sufficient.

In order to comply with this legal requirement, St. Patrick's Loreto Primary School 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.

The process of determining the Records Retention Schedule was carried out by reviewing current legislation. The principles of making good record retention decisions can be summarised as:

- Avoiding trying to accommodate every conceivable need;
- Retain information if it is likely to be needed in the future and if the consequences of not having it would be substantial;
- Be conservative i.e. avoid inordinate degrees of risk;
- Ensure systematic disposal of records immediately after their retention period expires or archive as determined;
- Base retention periods on the required legislation; and
- Apply common sense.

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 Statute 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 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	Final Disposition	Retention Comments
Registers/Roll books	N/A	Indefinitely. Archive when class leaves + 2 yrs
Records relating to pupils/students	Final Disposition	Retention Comments
Enrolment Forms (for pupils admitted to the school)	Confidential shredding/deletion	Student reaching 18 years + 7 years. 18 is age of majority + 7 years (6 years in which to take a claim against school, + 1 year for proceedings to be served on the school)
Pupil transfer forms (Applies from one school to another)	As above	As above
In-school standardised test results & SEN assessments	As above	As above
End of term/year reports	As above	As above
Disciplinary notes	As above	As above
School tours/trip records (including permission slips, itinerary reports)	As above	As above

Sensitive Personal Data Students	Final disposition	Retention Comments
Section 29 appeal records (for pupils enrolled in the school)	Confidential shredding/deletion	Student reaching 18 years + 7 years. 18 is the age of majority (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Accident reports	As above	As above
Records of complaints made by parents/guardians	Confidential shredding or N/A, depending on the nature of the records.	Depends entirely on the nature of the complaint but no longer than is necessary for the purpose of recording. If complaint is of a more mundane nature (e.g. misspelling of child's name, parent not contacted to be informed of parent-teacher meeting etc.), retention as above.
Enrolment forms where child not enrolled/ refused enrolment	Confidential shredding/deletion	Two years after non-admission, to provide time for review/appeal process
Psychological assessments	N/A	Never destroy
SEN files, reviews, correspondence & IEPs	N/A	Never destroy
Child protection records	N/A	Never destroy

Staff personnel files (whilst in employment)	Final Disposition	Comments
e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, staff training records 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/deletion	As above
Qualifications	As above	As above
References	As above	As above

Interview: database of applications (section which relates to employee only)	As above	As above
Selection criteria	As above	As above
Interview board marking scheme & board notes	As above	As above
Interview board panel recommendation	As above	As above
Recruitment medical	As above	As above
Garda Vetting outcome	As above	Record of outcome retained for 12 months. School to retain reference number & disclosure date on file, which can be checked with An Garda Síochána in the future.
Job specification/ description	As above	As above
Contract/Conditions of employment	As above	As above
Probation letters/forms	As above	As above
POR app & correspondence (if successful)	As above	As above
Leave of absence applications	As above	As above
Allegations/complaints	As above	As above Please note relevant DES Circular re Disciplinary Procedures in relation to period of time for which a warning remains "active" on an employee's record.
Grievance and Disciplinary records	As above	As above Please note relevant DES Circular re Disciplinary Procedures in relation to period of time for which a warning remains "active" on an employee's record.
Job share	As above	As above
Career break	As above	As above
Maternity leave	As above	As above
Paternity leave	As above	As above or for 2 years after retirement/ resignation (whichever greater)
Parental leave	As above	Retain for minimum of 8 years or as above
Parent's leave	As above	Retain for minimum of 8 years or as above
Force Majeure leave	As above	Retain for minimum of 8 years or as above
Carers Leave	As above	Retain for minimum of 8 years or as above
Working Time Act (attendance hours, holidays, breaks)	As above	Retain for minimum of 3 years or as above

Occupational Health Records	Confidential Shredding	Comments
Sickness absence records/certificates	Confidential shredding Or do not destroy	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to/in connection with individual's school duties, in which case, do not destroy.
Pre-employment medical assessment	As above	As above
Occupational health referral	As above	As above
Correspondence re retirement on ill-health grounds	As above	As above
Medical assess/ referrals	As above	As above

Sick leave records (sick benefit forms)	As above	In the case of audit/refunds as above
Accident/injury reports	As above	Retain for 10 years or as above

Other school based reports/minutes	Final Disposition	Comments
Payroll and taxation	Confidential shredding/ retained indefinitely	Revenue Commissioners require records be kept for at least 6 years after the end of the tax year. Records must be made available for inspection by authorised Revenue Commissioner officers or of Dept. of Social Protection. Note: The DE 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.
Audited accounts	N/A	Indefinitely
Invoices/ back-up records/ receipts	Confidential shredding/ deletion	Retain for 7 years

Board of Management Records	Final Disposition	Comments
Board agenda and minutes	N/A	Indefinitely. Store securely on school property
Principal's monthly report including staff absences	N/A	Indefinitely. Administrative log 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".
School closure	Transfer	On school closure, school to liaise with Patron. Decommissioning exercise should take place with respect to archiving and recording data.

Other school based reports/minutes	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 & where images/ recordings are retained to investigate those issues.

Recruitment Process Unsuccessful Candidate Records	Final disposition	Comments
Note: these retention periods apply to unsuccessful candidates only.	Confidential shredding / deletion	18 months from close of competition: 12 months plus 6 months for Workplace Relations Commission to inform school that claim is being taken.
Candidate applications/ CVs called for interview	As above	As above
Database of applications	As above	As above
Selection criteria	As above	As above
Applications of candidates not shortlisted	As above	As above
Unsolicited job applications	As above	As above
Candidates shortlisted but unsuccessful at interview	As above	As above

Successful candidates who do not accept offer	As above	As above
Interview board marking scheme & board notes	As above	As above
Panel recommendation by interview board	As above	As above

Government Returns	Final Disposition	Comments
Any returns which identify individual members of the school community	Confidential shredding/ retained indefinitely	Depends on return. If it relates to pay/pension/benefits of staff, keep indefinitely as per DE guidelines. If it relates to student information, e.g. October Returns, Annual Census etc., "Student Records" guidelines apply.

Superannuation /Pension /Retirement records	Final Disposition	Comments
Records of previous service (incl. prev. correspondence)	N/A	DE advises that these should be kept indefinitely.
Pension calculation	Confidential shredding/ deletion	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 longer)
Pension increases	As above	As above
Salary claim forms	As above	As above

APPENDIX 3: REFERENCE SITES

Data Protection Act 2018 <http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html>

General Data Protection Regulation (GDPR official text) 2016 <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

General Data Protection Regulation (GDPR unofficial web version) 2016 <https://gdpr-info.eu/>

GDPR for Schools website <https://gdpr4schools.ie/>

Data Protection for Schools <http://dataprotectionschools.ie/en/>

Irish Data Protection Commission <https://www.dataprotection.ie/>

Data Breach Report <https://forms.dataprotection.ie/report-a-breach-of-personal-data>

European Data Protection Board (EDPB) <https://edpb.europa.eu/>

EDPB Guidelines, Recommendations and Best Practices on GDPR https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

PDST Technology in Education <https://www.pdsttechnologyineducation.ie>

Cyber Security Centre (Ireland) <https://www.ncsc.gov.ie/>

Cyber Security Centre (UK) <https://www.ncsc.gov.uk/>

School Broadband Programme <https://www.pdsttechnologyineducation.ie/technology-infrastructure/schools-broadband-programme/>