



APPENDIX 1

The 8 Rules of Data Protection

- 1. Obtain and process information fairly**
- 2. Keep it only for one or more specified, explicit and lawful purpose**
- 3. Use and disclose it only in ways compatible with these purposes**
- 4. Keep it safe and secure**
- 5. Keep it accurate, complete and up-to-date**
- 6. Ensure that it is adequate, relevant and not excessive**
- 7. Retain it for no longer than is necessary for the purpose or purposes**
- 8. Give a copy of his/her personal data to that individual on request**



APPENDIX 2

Link to: [EU Data Protection Directive 95/46/EC](#)

Place your cursor over the link above, press ctrl and left click your mouse to follow the link.



APPENDIX 3

Your rights as a data subject

1. **Right to have your data processed in accordance with the Data Protection Acts**
to have your personal information obtained and processed fairly, kept securely and not unlawfully disclosed to others
2. **Right to be informed**
to know the identity of the data controller and the purpose for obtaining your personal information
3. **Right of access**
to get a copy of your personal information
4. **Right of rectification or erasure**
to have your personal information corrected or deleted if inaccurate
5. **Right to block certain uses**
to prevent your personal information being used for certain purposes
6. **Right to have your name removed from a direct marketing list**
to stop unwanted mail
7. **Right to object**
to stop some specific uses of your personal information
8. **Employment rights**
not to be forced into accessing personal information for a prospective employer
9. **Freedom from automated decision making**
to have a human input in the making of important decisions relating to you
10. **Rights under Data Protection and Privacy in Telecommunications Regulations**
to prevent your phone directory entry details from being used for direct marketing purposes



APPENDIX 4

Fair Processing

Fair Processing of personal data

Section 2A of the Acts details a number of conditions, at least one of which must be met, in order to demonstrate that personal data is being processed fairly. These conditions include that the data subject has consented to the processing, or that the processing is necessary for at least one of the following reasons:

1. The performance of a contract to which the data subject is party, or
2. In order to take steps at the request of the data subject prior to entering into a contract, or
3. In order to comply with a legal obligation (other than that imposed by contract), or
4. To prevent injury or other damage to the health of the data subject, or
5. To prevent serious loss or damage to the property of the data subject, or
6. To protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged, or
7. For the administration of justice, or
8. For the performance of a function conferred on by or under an enactment or,
9. For the performance of a function of the Government or a Minister of the Government, or
10. For the performance of any other function of a public nature performed in the public interest by a person, or
11. For the purpose of the legitimate interests pursued by a data controller except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject

Fair processing of sensitive personal data

If processing sensitive data, you must satisfy the requirements for processing personal data set out above along with at least one of the following conditions (set out in section 2B of the Acts):

1. The data subject has given explicit consent, or
2. The processing is necessary in order to exercise or perform a right or obligation which is conferred or imposed by law on the data controller in connection with employment, or
3. The processing is necessary to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where consent cannot be given, or the data controller cannot reasonably be expected to obtain such consent, or
4. The processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld, or
5. The processing is carried out by a not-for-profit organisation in respect of its members or other persons in regular contact with the organisation, or
6. The information being processed has been made public as a result of steps deliberately taken by the data subject, or



DATA PROTECTION POLICY

7. The processing is necessary for the administration of justice, or
8. The processing is necessary for the performance of a function conferred on a person by or under an enactment, or
9. The processing is necessary for the performance of a function of the Government or a Minister of the Government, or
10. The processing is necessary for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights, or
11. The processing is necessary for medical purposes, or
12. The processing is necessary in order to obtain information for use, subject to, and in accordance with, the Statistics Act, 1993, or
13. The processing is necessary for the purpose of assessment of or payment of a tax liability, or
14. The processing is necessary in relation to the administration of a Social Welfare scheme



APPENDIX 5

Consent

Where consent is the basis for provision of personal data (e.g. data required to join sports team/ after-school activity/or optional school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes. Each school will require a clear, affirmative action e.g. ticking of a box/signing a document, to indicate consent. Consent can be withdrawn by data subjects in these situations

To ensure that the school's practices are open and transparent and to obtain data fairly the data subject must, at the time the personal data is being collected, be made aware of:

- a. the name of the data controller (i.e. School BoM)
- b. the purpose/rationale for collecting the data and any secondary uses of their personal data which might not be obvious to them
- c. the persons or categories of persons to whom the data may be disclosed e.g.
 - 1) DES
 - 2) other third parties operating in the education and welfare sphere e.g. NCSE, TÚSLA, NEPS, SESS, the HSE, TUSLA, An Garda Síochána
 - 3) other third parties with whom the School contracts, such as cloud-based school administration software companies, accountants, insurance companies, lawyers, etc.
- d. whether replies to questions asked are obligatory and the consequences of not providing replies to those questions
- e. the existence of the right to access their personal data
- f. the right to rectify their data if inaccurate or processed unfairly
- g. any other information which is relevant so that processing may be fair and to ensure that the data subject has all the information that is necessary to facilitate their awareness of how their data will be processed

Where you use application forms or standard documentation in school for enrolment or other purposes, you should explain your purposes/uses etc. clearly on such forms or documentation

No age limit is associated with consent. However, it is important that the data subject appreciates the nature and effect of such consent. Therefore, different ages might be set for different types of consent. Where a person is unlikely to be able to appreciate the nature or effect of consent, by reason of physical or mental incapacity or age, then a parent, grandparent, uncle, aunt, brother, sister or guardian may give consent on behalf of the data subject. These are the only circumstances in which a third party may give consent on behalf of a data subject

FAIR OBTAINING: TEST YOURSELF

When people are giving you information, you should be able to answer YES to the following questions:-

1. do they know what information you will keep about them?
2. do they know the purpose for which you keep and use it?



DATA PROTECTION POLICY

3. do they know the people or bodies to whom you disclose or pass it?

In general, the fair obtaining principle requires that every individual about whom information is collected for holding will be aware of what is happening



APPENDIX 6

Third party service agreement

In accordance with the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation (GDPR), the BoM of *St. Tola's N.S.* requires this written third party service agreement to be in place with all our data processors

The GDPR requires that the BoM shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of GDPR and thus ensure the protection of the rights of the data subject

The BoM of *St. Tola's N.S.* as data controller imposes the following minimum obligations on you as data processor:

1. To act only on the documented instructions of the data controller i.e. the BoM of *St. Tola's N.S.* with regard to the subject-matter, the types of personal data processed, the documented purposes of the processing and the duration of the processing
2. To comply with the obligations imposed on data controllers by the Data Protection Acts 1988 to 2018 and the GDPR in order to ensure that appropriate steps are taken to ensure the confidentiality of the personal data being processed and to guard against the accidental destruction, damage or loss of personal data
3. To provide sufficient guarantees in respect of technical security measures and organisational measures governing the processing of the school's data
4. To provide an indemnity to the school Board of Management (BoM) for any breaches of the above legal conditions
5. To commit to the provision of assistance where appropriate to enable the school Board to comply with a data subject access request
6. To immediately contact the school principal Eileen Smyth (087 778 96 58), where there are any data security breaches in the data processor's company in order to facilitate the school BoM, as data controller, to take the required action in accordance with the GDPR regarding the data breach
7. To comply with the requirements of the Data Protection Policy of *St. Tola's N.S.* attached hereto
8. On termination of the contract between the data processor and the BoM of *St. Tola's N.S.*, all personal data held by the data processor must be returned to the Board as data controller or in the alternative, it must be entirely deleted from the data processor's systems and files



DATA PROTECTION POLICY

9. To make available to the controller (BoM) all information necessary to demonstrate compliance with the obligations of the GDPR and to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller

10. If the processor believes that any instruction it receives from the controller is in breach of the GDPR, the processor shall immediately inform the controller

(This agreement should be signed by the Data Processor and the BoM of the school and copies retained by both)

St. Tola's N.S. Killulagh, Delvin, Co. Westmeath or by email to st.tolasnews@hotmail.com



APPENDIX 7

Link to: [**REPORTING A DATA BREACH**](#)

Place your cursor over the link above, press ctrl and left click your mouse to follow the link.



DATA PROTECTION POLICY

APPENDIX 8

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 PROTECTION POLICY

Data Access Request:

I, [name] wish to make an Access Request for a copy of personal data that ST. TOLA'S N.S. 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 drivers license. 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 *Fr. S. Heaney, Parochial House, Delvin, Co. Westmeath*



APPENDIX 9

PRACTICAL STEPS TOWARDS GDPR

Compliance for further details of each area

In order to comply with GDPR, every BoM should ensure that

- a) they are aware of what data they currently hold and the reasons why they are processing it on an on-going basis
- b) the relevant School Staff are fully trained for their roles in relation to GDPR
- c) all School Staff are fully aware of the importance of Data Protection and that the school is a Data Protection Sensitive and Aware institution
- d) that all relevant Policies and Procedures are in place and embedded

On a practical level, this will require the BoM to complete the following: -

Data Audit

It is important that the BoM is aware of all the Data it holds, collects and processes. This will be the first task.

- a) List all of the types of data currently held by the school – See Draft School Data Protection Policy section on Personal Data
- b) Identify the location of storage of each type of Data
- c) Identify the legal basis for processing each type of Data
- d) Identify all Data Processing operations currently being carried out on that data: -
 - i. Who processes the Data – may be more than one person?
 - ii. Who has access to the Data?
 - iii. Security arrangements for the storage of the Data?
 - iv. Availability of the Data to the Data Subject, if required?
- e) List all of the Data Processors contracted by the BoM to process data on its behalf e.g. Aladdin, Databiz, School Accounting etc.
- f) Security of the Data while under the control of the BoM

Staff Training

The BoM must ensure that all School Staff are aware of the concept and practice of Data Protection as it applies to them in the course of their work. The contents of this Resource Bundle, Privileged Access Management Systems (**PAMS**) in particular, could form the basis for such training – as it applies to the particular school e.g. not all schools have CCTV. The object of this training will be to ensure that all School Staff become conscious of Data Protection and implement it in the course of their work

Embedding of a DP Culture

In order to ensure the success of DP training, the BoM must endeavour to inculcate a culture of awareness of DP within the school community. To achieve this the BoM needs to have a plan for training in and promotion of DP among School Staff, Parents and the BoM itself. It could take the



DATA PROTECTION POLICY

form of regular discussions on DP and how it is being implemented in the school at BoM meetings, at Parent Council meetings and at Croke Park hours

Policies, Agreements and Notifications

1. The BoM is advised to have a comprehensive School Policy on Data Protection – **PAM (Privileged access management)**. This should be devised in consultation with Staff and Parents, passed by the BoM and reviewed as required or at least every two years
2. The BoM is required to have a Written Service Agreement – **PAM** - with each Data Processor contracted by the BoM to process data on its behalf
3. Where a BoM has deployed CCTV, it is advised to have a separate CCTV Policy– **PAM**. There is also a requirement to post notifications in relation to CCTV at each camera's location
4. The Data Protection Commissioner recommends that a Privacy Statement – **PAM** - be placed in a reasonably obvious position on the website homepage

Administration Forms

Schools use Administration Forms e.g. Enrolment Forms, BoM Election Ballot Papers, Permission to use Photographs of a child etc. to assist in the smooth running of the school. In the main these Forms gather information which is then processed by the BoM or by a Data Processor on behalf of the BoM. In order to reassure Data Subjects that the BoM is following Fair Processing procedures, as is required by the Data Protection Legislation, it is important to ensure that all such forms contain a clear and specific rationale for the collection of such Data. Data Subjects have the right to know

1. what Data is being processed
2. the reasons for that processing
3. the name of the Data Controller who is responsible for the processing of their Data

Procedures and Routines

Each BoM should establish clear Procedures and Routines around the collection, processing, storage and disposal of Data under its control. It should also establish Procedures and Routines for engaging with Data Subjects who wish to exercise their rights under Data Protection Legislation. These Procedures and Routines should clearly outline:-

Collection and Processing of Data

The procedure for collection of Data – Forms used, follow up phone calls etc.

Procedures for dealing with Data Subjects who do not wish to provide Data which the BoM is legally authorised to collect

The personnel authorised by the BoM to collect such Data

The personnel authorised to access the Data

Processing

The procedure for processing the collected Data – whether within the school or by a Data Processor



DATA PROTECTION POLICY

Storage

The BoM must be aware of all electronic devices on which the Data is stored

The BoM must ensure that the Data on each of these devices is secure in event that the device is stolen or lost

The BoM must ensure that the School Employee who controls the electronic device is fully aware of his/her obligations in regard to the protection of the Data on their device

The BoM must ensure that all physical Data is properly stored in a secure filing system

The BoM must ensure that all Data stored physically or electronically is accessible to the Data Controller

Disposal

The BoM should have a clear procedure for the disposal of Data once the Retention Period – **PAM** - for such Data is reached. The BoM should also ensure that all School Staff are conscious of the safe disposal of any item, physical or electronic, containing Personal Data. This might require the purchasing of a shredder or the collection of sensitive material in a safe location for transport to an industrial shredder on a regular basis



DATA PROTECTION POLICY

APPENDIX 10

DATA AUDIT

Legal basis for processing each data type

Type of Data	Storage & Security of this Data	Legal Basis for Processing this Data
Enrolment Forms	Filing Cabinet in principal's Office	Dept. of Education requirement
Pupil Birth Certificates & Baptismal Certificate	Filing cabinet in Principal's office	Proof of age & for further sacraments to be received
Contact details of pupils and their parents	Filing cabinet in principal's office and Aladdin	Covid-19 critical incident information
Staff contact details and emergency contacts	Filing cabinet in principal's office and in general office and Aladdin	Covid – 19 critical incident information
Staff CVs, applications, medical certs, other	Filing Cabinet in principal's Office	Record of staff information as per Dept. pf Education
Educational Reports (<i>Psychological, O.T., Speech & Language, ASD, Other</i>)	Filing Cabinet in Principal's office	Support educational provision
Pupil Reports by teachers	Filing Cabinet in Principal's Office	Record of pupil attainment
Pupil Profile	Filing Cabinet in principal's Office	Record of pupil attainment
Teacher's Pupil Assessment File	Teacher's classroom locked filing cabinet	Record of pupil attainment
Standardised Test Results	Filing Cabinet in principal's office and SEN room	Record of pupil attainment
Pupil Screening Tests and information	Filing Cabinet in SEN Room & copies in principal's office	Support educational provision
Aladdin – Pupil Attendance	On-line	Record of Pupil Attendance under Dept. Guidelines
POD online system	Dept. of Education, Aladdin	Dept. of Education
BOM Ballot Papers	Stored in General Office	Dept. of Education Handbook Rules for Primary Schools
Minutes of BOM Meetings	Held in filing cabinet in principal's office	As per Rules for Schools / BOM Handbook
School/ Secretary's Diary	Held in General Office locked filing Cabinet	As a record of school business for 1 year
Principal's diary	Filing cabinet in principal's office	Record of day-to-day procedures and duties
Parent/ pupil Address Book	Held in General Office locked filing Cabinet	As a back-up system to Aladdin Schools



DATA PROTECTION POLICY

Old Roll Books	Held in Principal's Office & in Store room	Retained as school records as per Dept. of Educ. guidelines
Treasurer's Payroll for ancillary staff	Held by the Treasurer in locked facility	Retained as financial record for 5 years
Copy of financial documents including invoices, receipts	Online	As a Backup system of financial records for 5 years
Record of petty cash	Held in locked filing cabinet in general office	Retained as financial record for 5 years
SAGE Data	Online	Retained as financial record for 5 years
Photograph of children's work	Online learning portfolio – SeeSaw. Can be printed off and stored in teachers locked classroom file.	Retained until child transitions to next class.
Photograph's of children participating in lessons and activities	Taken on a specific school device – mobile phone/ assigned tablet and stored on school laptops backed up to the school OneDrive	Retained until child transitions to next class.
Samples of School work for assessment purposes	Stored in teachers locked classroom file.	Retained until end of school year and sent home with child.

Data Processing Personnel & Systems

Type of Data	Processor of this Data/ Access to this Data	Basis for personnel processing the data
Enrolment Forms	Principal / Secretary	Dept. of Education Entry on POD
Birth Certificate & Baptismal Certificates	Principal/ Secretary (POD) Fr. Heaney	Proof of age & proof for further sacraments to be received
Contact details of pupils and their parents	Principal, secretary and HSE contact tracing team	Comply with HSE Guidelines on Covid-19 critical incident
Pupil Reports by teachers	Principal Classroom Teachers SEN Teachers	Supporting pupil attainment
Pupil Profiles	Principal Classroom Teachers SEN Teachers	Supporting pupil attainment
Teacher's Pupil Assessment File	Classroom Teachers	Record of pupil attainment
Standardised Test Results	Principal, Deputy Principal & SEN team	Record of pupil attainment
Pupil Screening Tests and information	SEN Team	Support educational provision



DATA PROTECTION POLICY

Aladdin – Pupil Attendance	Principal Classroom Teachers Secretary	Analysis & recording of Pupil Attendance under Dept. Guidelines
Staff CVs, applications, medical certs, other	Principal	Comply with Dept. pf Education
Staff contact details and emergency contacts	Principal Secretary	Comply with HSE guidelines on Covid – 19 critical incident
POD online system	Principal Secretary	Comply with Dept. of Education
BOM Ballot Papers	Chairperson, BOM Principal Deputy Principal	Dept. of Education Handbook Rules for Primary Schools
Minutes of BOM Meetings	Chairperson, BOM Principal & Deputy Principal	As per Rules for Schools / BOM Handbook
School/ Secretary’s Diary	Secretary Principal & Deputy Principal	As a record of school business for 1 year
Principal’s Day book	1 academic year after the year of use for reference	As a daily record of work
Parent/ pupil Address Book	Principal, Secretary, Teachers & SNAs	As a contact & back-up system to Aladdin Schools
Old Roll Books	Principal & Deputy Principal	Retained as school records as per Dept. of Educ. guidelines
Treasurer’s Payroll for ancillary staff	Treasurer	Retained as financial record for 5 years
Copy of financial documents including invoices, receipts	Treasurer, principal, secretary	As a Backup system of financial records for 5 years
Record of petty cash	Treasurer, principal, secretary	Retained as financial record for 5 years
SAGE Data	Treasurer, principal, secretary	Retained as financial record for 5 years
Photograph of children’s work	Online learning portfolio – SeeSaw. Can be printed off and stored in teachers locked classroom file.	Retained until child transitions to next class.
photograph’s of children participating in lessons and activities	Taken on a specific school device – mobile phone/ assigned tablet and stored on school laptops backed up to the school OneDrive	Retained until child transitions to next class.
Samples of School work for assessment purposes	Stored in teachers locked classroom file.	Retained until end of school year and sent home with child.



DATA PROTECTION POLICY

Disposal of Data at the end of the retention period:

Data	Retention Period	Disposal
Enrolment Forms	Until child reaches 25 years	Shredded
Birth Certificate (Copy)	Retained with the application form	Shredded
Baptismal Certificate (Copy)	3 months prior to sacramental ceremony	Shredded
Educational Reports (<i>Psychological, O.T., Speech & Language, ASD, Other</i>)	Until child reaches 25 years	Shredded
Pupil Reports by teachers	Until child reaches 25 years	Shredded
Pupil Profile	Until child reaches 25 years	Shredded
Teacher's Pupil Assessment File	Until child reaches 25 years	Shredded
Standardised Test Results	Until child reaches 25 years	Shredded
Pupil Screening Tests and information	Until child reaches 25 years	Shredded
Aladdin – Pupil Attendance	Annually	Deleted by Aladdin
Staff CVs, applications, medical certs, other	Retained for 1 year after they leave St. Tola's N.S.	Shredded
POD online system	Retained by the Dept. of Education	POD system updated each year by the Dept. of Educ.
BOM Ballot Papers	Retained for the 4-year period of the Board's service	Shredded
Minutes of BOM Meetings	10 Years	As per Rules for Schools / BOM Handbook
School/ Secretary's Message Book	1 academic year after the year of use for reference	Shredded
Principal's Day book	1 academic year after the year of use for reference	Shredded
Parent/ pupil Address Book	8 years	Old names/ numbers are removed on leaving school
Old Roll Books	Indefinitely	Retained as school records as per Dept. of Educ. guidelines
Treasurer's Payroll for ancillary staff	Treasurer	Shredded after 5 years
SAGE Data	Treasurer, principal, secretary	Retained as financial record for 5 years
Photograph of children's work	Online learning portfolio – SeeSaw. Can be printed off and stored in teachers locked classroom file.	Retained until child transitions to next class.
Photograph's of children participating in lessons and activities	Taken on a specific school device – mobile phone/ assigned tablet and stored on	Retained until child transitions to next class.



DATA PROTECTION POLICY

	school laptops backed up to the school OneDrive	
Samples of School work for assessment purposes	Stored in teachers locked classroom file.	Retained until end of school year and sent home with child.

All filing Cabinets are locked at all times and office areas are locked when school is closed.

ACTIONS:

Data Processors which are contracted by the Board of Management must supply a service agreement:

1. Aladdin.schools (Written Service Agreement in place)
2. Textaparent

Security of the Data while under the control of the BOM

1. New filing cabinets to be purchased for storage of pupil personal data documents which must be stored from leaving 6th class until the person is 21yrs.
2. A filing cabinet with lock is provided in each classroom
3. CCTV Recording unit to be replaced and the whole system to be moved to the Secretary's Office. This system may need to be upgraded (Merrion Security notified)
4. Shredder purchased
5. All parents to be given a new GDPR Consent Form September 2018 consenting/ not consenting to photos or other media images usage

Data Protection Policy is in place & CCTV Monitoring Policy and Mobile Phone/ Device Policy

Policies relative to Data Protection:

1. St. Tola's Data Protection & Record-keeping Policy (Ratified October 2017)
2. CCTV Monitoring Policy (Ratified May 16th 2018)
3. Mobile Phone & Device Use (Ratified May 16th 2018)



DATA PROTECTION POLICY

APPENDIX 11
RETENTION PERIOD

Data Retention Periods for schools

Pupil Related	Retention Periods
School Register/Roll Books Enrolment Forms Disciplinary notes Test Results – Standardised Psychological Assessments etc. SEN Files/IEPS Accident Reports Child Protection Reports/Records S.29 Appeals	Indefinitely Hold until Pupil is 25 Years Never Destroy Hold until pupil is 25 Years Never Destroy Never Destroy Never Destroy Never Destroy Never Destroy
Interview Records	
Interview Board Marking Scheme Board of Management notes (for unsuccessful candidates)	18 months from close of competition plus 6 months in case Equality Tribunal needs to inform school that a claim is being taken
Staff Records	
Contract of Employment Teaching Council Registration Vetting Records Accident/Injury at work Reports	Retention for duration of employment + 7 years (6 years to make a claim against the school plus 1 year for proceedings to be served on school)



DATA PROTECTION POLICY

BoM Records	
<p>BOM Agenda and Minutes</p> <p>CC TV Recordings</p> <p>Payroll & Taxation</p> <p>Invoices/receipts</p> <p>Audited Accounts</p>	<p>Indefinitely</p> <p>28 days normally. In the event of criminal investigation – as long as is necessary</p> <p>Revenue require a 6-year period after the end of the tax year</p> <p>Retain for 7 Years</p> <p>Indefinitely</p>
<p><i>Why, in certain circumstances, does the Data Protection Commission recommend the holding of records until the former pupil has attained 25 years of age?</i></p> <p><i>The reasoning is that a pupil reaches the age of majority at 18 years and that there should be a 6-year limitation period in which it would be possible to take a claim against a school, plus 1 year for proceedings to be served on a school. The Statute of Limitations imposes a limit on a right of action so that after a prescribed period any action can be time barred.</i></p>	



APPENDIX 12

WEBSITE PRIVACY STATEMENT

St. Tolas is committed to preserving the privacy of all visitors to <https://www.sttolasdelvin.com/> (“our website”). This privacy statement relates to our practices in connection with our website and is designed to assist you in understanding how we collect, use and safeguard the personal information you provide to us and to assist you in making informed decisions when using our site and our services. St. Tolas fully respects your right to privacy. We will not collect personal information/personal data about you when you visit our website unless you choose to provide that information using the “*Contact us*” form.

By using this site, you consent to the collection and use of your information under the terms of this privacy statement which is in accordance with the Data Protection Acts 1988 to 2018, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 and the EU General Data Protection Regulation (GDPR). Please read the following privacy statement to understand how we use and protect the information that you choose to provide to us.

What Information Do We Collect?

When you visit our website you may provide us with two types of information:

- Personal information you knowingly choose to disclose that is collected on an individual basis, and
- Statistical web site use information collected on an aggregate basis as you and others browse through our website(s)

INFORMATION, PERSONAL AND NON-PERSONAL, YOU CHOOSE TO PROVIDE

Email address

When you visit our website you may wish to provide certain information about yourself, such as when you complete our “*Contact Us*” form. **St. Tolas** does not collect any personal data about you on this website, apart from the information which you volunteer to send us in the “*Contact Us*” form

Web Site Use Information

Where you visit our website, certain non-personal data is available to us through our internet service provider. This non-personal data is collected on a statistical, aggregate, non-individual basis. This information may include the IP address from which you access our website, the type of internet browser used to access our website, the type of operating system used to access our website, the “top-level” domain name used (ie, .com, .org, etc.), the date and time of your visit to our website and the number of pages you visited on our website

How Do We Use the Information That You Provide to Us?

Any information, which you provide using the “*Contact Us*” form, is not made available to any third parties and is only used by **St. Tolas** in line with the purposes for which you provided it (e.g. to contact



DATA PROTECTION POLICY

you and answer any queries which you have raised in the “*Contact Us*” form or to address any other feedback which you send us in the “*Contact Us*” form)

Disclosure to Other People:

We do not disclose, sell or distribute any personal information which you send to us to any third parties. We may pass aggregate information on the usage of our site to third parties, but this will not include information that can be used to identify you. Your personal data may also be anonymised and used for statistical purposes. Unless required to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

IP Addresses:

An IP address is a number that is assigned to your computer automatically when you use the internet. When you visit any web page in our website, our servers log your IP address. We may use your IP address to help diagnose problems with our server and to administer our website. Your IP address is also used to help identify you and to gather broad demographic information.

What Are Cookies?

Cookies are a feature of web browser software that allows web servers to recognise the computer used to access a website. Cookies are small pieces of data that are stored by a user's web browser on the user's hard drive

Cookies can remember what information a user accesses on one web page to simplify subsequent interactions with that web site by the same user or to use the information to streamline the web page and to complete commercial transactions over the Internet. Cookies should make your online experience easier and more personalized

Our website uses cookies to keep track of your access to the site. By using our website, you agree that we can place these types of cookies on your device

Your browser will give you the option of preventing websites using cookies, or deleting cookies that have been accepted. Your browser's help service or help manual will show you how this is done. If you do not want your browser to accept cookies, you can “turn off” the cookie acceptance setting on your browser setting. However, you must note that this may stop our website from working properly on your device. If you do not change your browser settings to refuse cookies, our website will issue cookies when you visit our website. If you continue to use our website, you agree and consent to our use of cookies on your device

Security

We employ security measures to protect your information from access by unauthorised persons and to guard against unlawful processing, accidental loss, destruction and damage and we will do our best to ensure that all records we hold remain secure in line with our obligations under Data Protection Acts 1988 to 2018. We take our security responsibilities seriously, employing appropriate physical and technical measures. We review our security procedures regularly.

Retention

We do not retain your personal data for longer than it is necessary for us to comply with the purpose for which you gave it to us. Any personal data which you provide to us using this website will be used in line with the purposes for which you provided it (e.g. to contact you and answer any queries which



DATA PROTECTION POLICY

you have raised in the “*Contact Us*” form or to address any other feedback which you send us in the “*Contact Us*” form) and after this purpose has been completed, we will delete your personal data.

Accessing Your Information

You are entitled to see the information we hold about you. On written request, we supply copies of your personal data, which you may have supplied to us using our website. If you wish to obtain copies of this personal data, you should write to the Board of Management of St. Tolas at Killulagh, Delvin, Co. Westmeath and ask that it provides you with an Access Request Form. Your request will be dealt with as soon as possible and will not take more than a month to process. If you discover that St. Tolas holds inaccurate information about you, you can request that we correct/delete that information.

Websites Linked to Our Website

Our website may, from time to time, contain links to and from third party websites. We are not responsible for the practices employed by websites linked to or from our website nor the information or content contained therein. Often links to other websites are provided solely as pointers to information on topics that may be useful to the users of our website

Please remember that when you use a link to go from our website to another website, our Privacy Policy is no longer in effect. Your browsing and interaction on any other website, including websites which have a link on our website, is subject to that website's own rules and policies. Please read over those rules and policies before proceeding

By using our website you consent to our collection and use of your personal information as described in this Privacy Policy. If we change our privacy policies and procedures, we will post those changes on our website to keep you abreast of any developments

Contacting Us

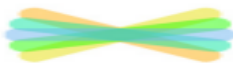
If you are concerned about how your personal data is processed by our website, please bring your concerns to our attention using the contact details below:

The Board of Management,
St. Tolas National School, Killulagh, Delvin, Co. Westmeath
or by email to st.tolasnews@hotmail.com



Appendix 13

Seesaw Privacy, Safety and Security



Protecting your privacy is fundamental to our mission and business. The following summarize our promises to you.

- We never sell your data or student data: We will never sell or rent your data or create profiles of Seesaw users to sell. Our business model is straightforward: we charge schools and districts for optional, additional features on top of our free product.
- We never advertise in Seesaw: We have no interest in advertising in Seesaw. Again, our business model is straightforward: we charge schools and districts for optional, additional features on top of our free product.
- We don't own the content you add to Seesaw: Students and their schools own the work added to Seesaw. If you'd ever like to save your content elsewhere or use a different product, you can download what you've added to Seesaw to your computer or mobile device. You can also delete your account at any time and we will permanently delete your account and all associated data within 60 days.
- Student work is private to the classroom by default: Teachers control what is shared and with whom. Unless teachers choose to share, no student work is visible outside of the classroom. Teachers can choose to invite family members to see the work their child has added to Seesaw or post some items more publicly (such as to a Seesaw blog)
- We use the latest security industry best practices to protect you: This means we do things like provide secure communication with our servers at all times, encrypt journal content at rest, and run regular 3rd party security audits to make sure your information is secure. Read more about how we keep student data safe at help.seesaw.me.
- We are transparent about our practices, and will notify you if things change: We strive to make our policies easy to understand. If anything substantial were to change with our privacy practices, we would let you know. The privacy policy and terms you agreed to will still apply unless you accept new terms.
- We are compliant with FERPA, COPPA and GDPR: Seesaw is compliant with these important laws so it's safe to use Seesaw in the classroom.

Read our full Privacy Policy on our website at seesaw.me/privacy.



Appendix 14

Dear Parents:

I am delighted to share with you that this school year our class will be using Seesaw (<http://seesaw.me>), a secure online journal where students can document and reflect on what they are learning in class. Your child will be able to add the things we work on (including photos, videos, worksheets, drawings and voice recordings) to their Seesaw journal and we can share them privately with you and other family members to view and comment on throughout the school year.

In order for your child to use Seesaw, the app needs your child's name in order to be able to associate work like their photos, videos or voice recordings with their account. Seesaw only uses this information to provide the service and doesn't advertise in Seesaw, create profiles of students, or share or sell your child's personal information or journal content. You can read more about their strong privacy promises here: <https://web.seesaw.me/privacy>.

Under an EU law called the General Data Protection Regulation (GDPR), in order for your child to use Seesaw, the school must get your consent. For more information on GDPR, please visit <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens>.

I hope that your child will enjoy using Seesaw to document and share their learning this year. Please sign below and return this permission slip so that your child can use Seesaw.

Please sign below and return the form.

I give consent for my child, listed below, to use Seesaw for class activities.

Student Name: _____

Parent Printed Name: _____

Parent Signature: _____ Date: _____



Appendix 15

Wix.com Privacy Policy

Wix.com cares deeply about the privacy of its visitors and users. To that end, this Privacy Policy (“Privacy Policy”) describes how Wix.com Ltd., together with its affiliated companies worldwide (“Wix”, “we”, “our”, or “us”), collect, use, and share your Personal Information, as well as an explanation of the data rights you may have in that Personal Information. This Privacy Policy applies to all Wix users, including unregistered visitors, registered users, and premium users (collectively, “Users”, “you”, or “your”), and to all Wix services, including our websites (including and any of its subdomains, the “Website”), web applications (“Wix Apps”), mobile applications (“Mobile Apps”), and related services (collectively, the “Services”). This Privacy Policy is not intended to override the terms of any contract you have with us, nor any rights you may have under other applicable data privacy laws.

Prior to accessing or using our Services, please read this policy and make sure you fully understand our practices in relation to your Personal Information. If you read and fully understand this Privacy Policy, and remain opposed to our practices, you must immediately leave and discontinue all use of any of our Services. If you have any questions or concerns regarding this policy, please contact us at .

2. What Personal Information do we collect

2.1. User Information:

To provide you the Services, we must collect Personal Information relating to an identified or identifiable natural person (“Personal Information”). We collect Personal Information you provide us, from your use of the Services, and from other sources. Here are the types of Personal Information we collect about you:

1. Information you provide us. When you register for our Services, purchase and/or register domain names, use any of our Services; and/or when you contact us directly by any communication channel (e.g., Wix’s support tickets, emails), you may provide us Personal Information, such as name, email address, phone number, payment information (for Users with Paid Services), information you include in your communications with us and with other users on our platform, and Personal Information contained in scanned identification documents (such as an ID card, driver’s license, passport, or official company registration documents).
2. Information we collect when you use the Services. When you visit, download, and/or use any of our Services, we may collect aggregated usage Personal Information, such as Visitors’ and Users’ browsing and ‘click-stream’ activity on the Services, session heatmaps and scrolls, non-identifying



DATA PROTECTION POLICY

Personal Information regarding the Visitor's or User's device, operating system, internet browser, screen resolution, language and keyboard settings, internet service provider, referring/exit pages, date/time stamps, etc

3. Information we collect from other sources. We may receive Personal Information about you from third-party sources, such as i) security providers, fraud detection and prevention providers for example to help us screen out users associated with fraud, ii) social media platforms, when you log-in or sign-up using your social media account, we may receive Personal Information from that service (e.g., your username, basic profile Personal Information) and in some cases, we may collect Personal Information from lead enhancement companies which help us to improve our service offering; iii) advertising and marketing partners in order to monitor, manage and measure our ad campaigns.

To provide our Services, we collect Personal Information about our Users.

The Personal Information comes from you when you visit or use our services, Personal Information we collect automatically, and Personal Information we collect from other sources.

2.2. Users of Users Personal Information

We may also collect Personal Information pertaining to visitors and users of our User's websites or services ("Users-of-Users"), solely for and on our Users' behalf (as further described in [Section 6](#) below).

2.3. Wix Jobs Applicant Information

We also collect information that is provided to us by Wix jobs candidates ("Applicants"), when they apply to any of the open positions published at, by e-mail or otherwise (as further described in [Section 15](#) below)

Why do We collect such Personal information

We use your Personal Information for the following purposes:

1. To provide and operate the Services;
2. .To further develop, customize, expand, and improve our Services, based on Users' common or personal preferences, experiences and difficulties;
3. To provide our Users with ongoing customer assistance and technical support;
4. To be able to contact our Users with general or personalized service-related notices and promotional messages (as further detailed in [Section 8](#) below);
5. To help us to update, expand and analyze our records to identify new customers;



DATA PROTECTION POLICY

6. To facilitate, sponsor, and offer certain contests, events, and promotions, determine participants' eligibility, monitor performance, contact winners, and grant prizes and benefits;
7. To analyse our performance and marketing activities;
8. To create aggregated statistical data and other aggregated and/or inferred information, which we or our business partners may use to provide and improve our respective services;
9. To provide you with professional assistance, only upon your request;
10. To enhance our data security and fraud prevention capabilities; and
11. To comply with any applicable laws and regulations.

We use your Personal Information for the purposes set out in Section 3 where:

1. Our use of your Personal Information is necessary to perform a contract or to take steps to enter into a contract with you (e.g. to provide you with a website builder, to provide you with our customer assistance and technical support);
2. Our use of your Personal Information is necessary to comply with a relevant legal or regulatory obligation that we have; or
3. Our use of your Personal Information is necessary to support legitimate interests and business purposes (for example, to maintain and improve our Services and the effectiveness of Wix by identifying technical issues), provided it is conducted in a way that is proportionate and that respects your privacy rights.

See More at <https://www.wix.com/about/privacy>



Appendix 16

Word Press.org - Privacy Policy

WordPress.org websites (collectively “WordPress.org” in this document) refer to sites hosted on the WordPress.org, WordPress.net, WordCamp.org, BuddyPress.org, bbPress.org, and other related domains and subdomains thereof. This privacy policy describes how WordPress.org uses and protects any information that you give us. We are committed to ensuring that your privacy is protected. If you provide us with personal information through WordPress.org, you can be assured that it will only be used in accordance with this privacy statement.

Website Visitors

Like most website operators, WordPress.org collects non-personally-identifying information of the sort that web browsers and servers typically make available, such as the browser type, language preference, referring site, and the date and time of each visitor request. WordPress.org’s purpose in collecting non-personally identifying information is to better understand how WordPress.org’s visitors use its website. From time to time, WordPress.org may release non-personally-identifying information in the aggregate, e.g., by publishing a report on trends in the usage of its website. WordPress.org also collects potentially personally-identifying information like Internet Protocol (IP) addresses. WordPress.org does not use IP addresses to identify its visitors, however, and does not disclose such information, other than under the same circumstances that it uses and discloses personally-identifying information, as described below.

Gathering of Personally-Identifying Information

Certain visitors to WordPress.org choose to interact with WordPress.org in ways that require WordPress.org to gather personally-identifying information. The amount and type of information that WordPress.org gathers depends on the nature of the interaction. For example, we ask visitors who use our forums to provide a username and email address.

In each case, WordPress.org collects such information only insofar as is necessary or appropriate to fulfill the purpose of the visitor’s interaction with WordPress.org. WordPress.org does not disclose personally-identifying information other than as described below. And visitors can always refuse to supply personally-identifying information, with the caveat that it may prevent them from engaging in certain website-related activities, like purchasing a WordCamp ticket.

All of the information that is collected on WordPress.org will be handled in accordance with GDPR legislation.

Protection of Certain Personally-Identifying Information

WordPress.org discloses potentially personally-identifying and personally-identifying information only to those of project administrators, employees, contractors, and affiliated organizations that (i) need to know that information in order to process it on WordPress.org’s behalf or to provide services available through WordPress.org, and (ii) that have agreed not to disclose it to others. Some of those employees, contractors and affiliated organizations may be located outside of your home country; by using WordPress.org, you consent to the transfer of such information to them.

WordPress.org will not rent or sell potentially personally-identifying and personally-identifying information to anyone. Other than to project administrators, employees, contractors, and affiliated organizations, as described above, WordPress.org discloses potentially personally-identifying and personally-identifying information only when required to do so by law, if you give permission to



DATA PROTECTION POLICY

have your information shared, or when WordPress.org believes in good faith that disclosure is reasonably necessary to protect the property or rights of WordPress.org, third parties, or the public at large.

If you are a registered user of a WordPress.org website and have supplied your email address, WordPress.org may occasionally send you an email to tell you about new features, solicit your feedback, or just keep you up to date with what's going on with WordPress.org and our products. We primarily use our blog to communicate this type of information, so we expect to keep this type of email to a minimum.

If you send us a request (for example via a support email or via one of our feedback mechanisms), we reserve the right to publish it in order to help us clarify or respond to your request or to help us support other users. WordPress.org takes all measures reasonably necessary to protect against the unauthorized access, use, alteration, or destruction of potentially personally-identifying and personally-identifying information.

Use of personal information

We use the information you provide to register for an account, attend our events, receive newsletters, use certain other services, or participate in the WordPress open source project in any other way.

We will not sell or lease your personal information to third parties unless we have your permission or are required by law to do so.

We would like to send you email marketing communication which may be of interest to you from time to time. If you have consented to marketing, you may opt out later.

You have a right at any time to stop us from contacting you for marketing purposes. If you no longer wish to be contacted for marketing purposes, please click on the unsubscribe link at the bottom of the email.

Legal grounds for processing personal information

We rely on one or more of the following processing conditions:

- our legitimate interests in the effective delivery of information and services to you;
- explicit consent that you have given;
- legal obligations.

Access to data

You have the right to request a copy of the information we hold about you. If you would like a copy of some or all your personal information, please follow the instructions at the end of this section.

All WordCamp attendee-provided data can be viewed and changed by the attendee via the Access Token URL that is emailed to confirm a successful ticket purchase.

WordPress.org user accounts can be edited by following these steps:

1. Visit <https://login.wordpress.org/>, and enter your username and password.
2. You will be redirected to https://profiles.wordpress.org/your_username.
3. Click the "Edit" link next to your username.

If you would like to request access to your account data, please follow these steps:

1. Visit <https://wordpress.org/about/privacy/data-export-request/>.
2. Enter your email address.
3. Click "Accept Declaration and Request Export".

Note: If you have a WP.org account, it's recommended you log in before submitting to associate your account with the request.



Retention of personal information

We will retain your personal information on our systems only for as long as we need to, for the success of the WordPress open-source project and the programs that support WordPress.org. We keep contact information (such as mailing list information) until a user unsubscribes or requests that we delete that information from our live systems. If you choose to unsubscribe from a mailing list, we may keep certain limited information about you so that we may honor your request.

WordPress.org will not delete personal data from logs or records necessary to the operation, development, or archives of the WordPress open-source project.

WordPress.org shall maintain WordCamp attendee data for 3 years to better track and foster community growth, and then automatically delete non-essential data collected via registration.

Attendee names and email addresses will be retained indefinitely, to preserve our ability to respond to code of conduct reports.

On WordCamp.org sites, banking/financial data collected as part of a reimbursement request is deleted from WordCamp.org 7 days after the request is marked paid. The reason for the 7-day retention period is to prevent organizers having to re-enter their banking details if a wire fails or if a payment was marked “Paid” in error. Invoices and receipts related to WordCamp expenses are retained for 7 years after the close of the calendar year’s audit, by instruction of our financial consultants (auditors & bookkeepers).

When deletion is requested or otherwise required, we will anonymise the data of data subjects and/or remove their information from publicly accessible sites if the deletion of data would break essential systems or damage the logs or records necessary to the operation, development, or archival records of the WordPress open-source project.

If you would like to request deletion of your account and associated data, please follow these steps:

1. Visit <https://wordpress.org/about/privacy/data-erasure-request/>.
2. Enter your email address.
3. Click “Accept Declaration and Request Permanent Account Deletion”.

Note: If you have a WP.org account, it’s recommended you log in before submitting to associate your account with the request.

Rights in relation to your information

You may have certain rights under data protection law in relation to the personal information we hold about you. In particular, you may have a right to:

- request a copy of personal information we hold about you;
- ask that we update the personal information we hold about you, or independently correct such personal information that you think is incorrect or incomplete;
- ask that we delete personal information that we hold about you from live systems, or restrict the way in which we use such personal information (for information on deletion from archives, see the “Retention of personal information” section);
- object to our processing of your personal information; and/or
- withdraw your consent to our processing of your personal information (to the extent such processing is based on consent and consent is the only permissible basis for processing).

If you would like to exercise these rights or understand if these rights apply to you, please follow the instructions at the end of this Privacy statement.



Third Party Links

Our website may contain links to other websites provided by third parties not under our control. When following a link and providing information to a 3rd-party website, please be aware that we are not responsible for the data provided to that third party. This privacy policy only applies to the websites listed at the beginning of this document, so when you visit other websites, even when you click on a link posted on WordPress.org, you should read their own privacy policies.

Aggregated Statistics

WordPress.org may collect statistics about the behavior of visitors to its websites. For instance, WordPress.org may reveal how many times a particular version of WordPress was downloaded or report on which plugins are the most popular, based on data gathered by `api.wordpress.org`, a web service used by WordPress installations to check for new versions of WordPress and plugins. However, WordPress.org does not disclose personally-identifying information other than as described in this policy.

Cookies

Additionally, information about how you use our website is collected automatically using “cookies”. Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This information is used to track visitor use of the website and to compile statistical reports on website activity.

Please see [our cookie policy](#) for more information about what cookies are collected on WordPress.org.

Privacy Policy Changes

Although most changes are likely to be minor, WordPress.org may change its Privacy Policy from time to time, and at WordPress.org’s sole discretion. WordPress.org encourages visitors to frequently check this page for any changes to its Privacy Policy. Your continued use of this site after any change in this Privacy Policy will constitute your acceptance of such change.

Contact

Please contact us if you have any questions about our privacy policy or information, we hold about you by emailing dpo@wordcamp.org.