Terenure College

Templeogue Road

Dublin 6W

School Roll Number: 60570H

Data Protection Policy

May 2019

Table of Contents

Data Protection Policy

Appendices

Terenure College Data Protection Policy

1. Introductory Statement

Terenure College is a Catholic school in the Carmelite tradition. The school aims to enable students to develop their full potential, provide a safe and secure environment for learning while promoting respect for the diversity of values, beliefs, traditions, languages and ways of life in society.

There are legitimate interests for compiling ***personal data***, including but not limited to, enabling pupils to develop to their full potential, employing members of staff, ensuring parents/guardians are contacted in the case of emergency or school closures, and informing parents/guardians of the child's educational progress.

This policy sets out the manner in which personal data should be protected by the school. It was formulated in consultation with staff and the Board of Management, in May 2019, in order to comply with existing ***Data Protection Acts*** and the EU General Data Protection Regulation (GDPR).

2. Scope

The school's Data Protection Policy applies to the keeping and processing of ***personal data***, both in manual and electronic form. It applies to all school staff, the Board of management, parents/guardians, students and others insofar as the measures under the policy relate to them.

3. Rationale

The school must process personal data to comply with its legal and statutory obligations under the broad remit of educational and workplace legislation.

Terenure College adopts a ***privacy by design*** approach to data protection. This policy outlines what sort of data is collected, why it is collected, for how long it will be stored, with whom it will be shared and the safe practices which are needed to safeguard individuals' personal data.

4. GDPR Rights and Principles

All processing of personal data must be conducted in accordance with the data protection principles while adhering to the ***data subject*** rights as set out in the relevant legislation.

4.1 Data Subject Rights

The individual rights under GDPR include:

1. **The right to be informed**. The individual should know the identity of the ***data controller*** and the purpose for which the personal information is obtained.
2. **The right of access**. The individual can access their personal data via a ***SAR (Subject Access Request)***.
3. **The right of rectification**. The individual may amend or correct personal information at any time.
4. **The right of erasure.** The individual has the right to be forgotten. This is subject to any statutory retention periods which may legitimise the purpose for retaining the data.
5. **The right to restrict processing**. The individual may request for their data to be restricted but the information will be still stored by the school.
6. **The right to data portability**. The individual may request the transfer of data to a second data controller such as another school.

4.2 Data Protection Principles

The school is responsible for and must be able to demonstrate compliance with the six principles of GDPR.

1. **Fair, transparent and lawful processing**. The data subject should know the type of data collected and the reason the school collects the data.
2. **Purpose limitation**. The school should only collect data for a specific purpose and keep only for as long as necessary.
3. **Minimisation of processing.** The school must only process data that is needed to achieve its processing purpose.
4. **Data accuracy**. The school must take every reasonable step to ensure the data they process is accurate and complete.
5. **Storage limitation**. The school should hold data in a form that identifies a data subject for as short a time as possible.
6. **Integrity and confidentiality**. The school must process data securely to safeguard against unauthorised/unlawful processing, accidental loss, destruction or damage.

5. Personal Data

The personal data records held by the school may relate to:

1. **Students** (See Appendix 2)

   Schools are expected to gather data about students through the enrolment process and/or through expressions of interest in relation to enrolment. This is legitimate for the purposes of providing educational services to students. Additional information may be collected from third parties, including former schools and through school activities and interaction(s) during the course of the student's time at school.

2. **Parents/Guardians** (See Appendix 3)
   Schools must also collect personal data about parents and guardians through the enrolment process or expressions of interest for enrolment. Additional data may be collected through interactions during the course of the student's time at school.
3. **Staff** (See Appendix 4)
   Schools are places of employment and so personal data is collected by the school in relation to all employees, including teachers, prior to and during the course of their employment at the school.
4. **Others** (See Appendices 5 and 6)

6. Location & Security

Manual records are kept in secure, locked filing cabinets in designated storage areas including administrative and management offices which are only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access. Digital records are stored on password-protected computers with adequate encryption and firewall software. For additional security, the school has a CCTV camera system and active burglar alarm installed on the premises.

7. Consent

In line with GDPR requirements, parents/guardians must give strict permission for:

1. The school to take photographs/videos of the student for use on the school website, twitter, the annual, etc, using authorised school cameras and videorecorders.
2. The school to contact the student via messenger services such as WhatsApp and/or Viber for the purpose of communicating extracurricular activities.

When obtaining written consent, clear and concise questions must be outlined on a form/application together with opt in opt out boxes.

Consent may be withdrawn by the parent/guardian at any time by resubmitting the form indicating the new level of consent.

8. Communication

Safe and secure measures should be taken when communicating with parents/guardians and students.

8.1 Email

- All correspondence made between staff and parents/guardians and/or students should be made through an official school email address, not a personal one.
- BCC (blind carbon copy) recipients when sending group emails.

8.2 Messenger Services – WhatsApp, Viber and Other.

- Messenger service communication may be required for certain school events such as for the organisation of sporting activities and school tours.
- Such communication requires an explicit opt-in, e.g., via a check box on a permission form. Such a form must be filled out by the parent/guardian.
- Photos and contact details should not be shared amongst members of a group. To ensure privacy, BCC message recipients.
- The default setting for some messenger providers may result in the automatic display of the profile photo together. This feature can be overwritten at any time by the student.
- Storage of the (encrypted) data is an issue for messenger service provider, not for the education institution. In that respect, service providers are expected to adhere to the law.
- No student should be contacted through details passed on by a third party.
- The content of the conversation thread should be confined to the purpose for which the group was set up.
- Messages and contact details should only be kept for a 'reasonable period until they are no longer useful'.

9. CCTV

CCTV is installed to ensure the safety and security of staff, students and visitors, and to safeguard school property and equipment. Signs which outline the location and purpose of CCTV use are displayed across the school. The retention period of recordings is 28 days after which the system automatically overwrites the images.

CCTV footage may be used for investigating behavioural incidences. Should any ***SAR*** be made in relation to footage, the recording should be redacted/pixelated before release, so that the only visible person is the relevant data subject. Clips which are subject to pixilation should be deemed to be relevant and short, typically seconds or minutes in length. Should the request for footage be excessive or unreasonable, a fee maybe incurred, and the request may be refused in which case the data subject should contact the ***Data Protection Commissioner***.

10. Related School Governing Policies

Relevant school policies which are already in place or which are being currently developed or reviewed shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed. These include the:

- Child Safeguarding Procedures.
- Anti-Bullying Policy.
- Code of Behaviour.

- SPHE Policy.
- Admissions Policy.
- School Excursions Policy.
- ICT Acceptable Usage Policy.
- Internet & Email Policy (Staff).

11. Roles and Responsibilities

As implementor of the Data Protection Policy, the principal must ensure that staff who handle or have access to personal data are familiar with their data protection responsibilities. In summary:

Individual	Responsibility
Board of Management	***Data Controller***
Principal	Implementor of the policy
Teaching personnel	Awareness, confidentiality
Administrative personnel	Security, confidentiality
IT personnel	Security, encryption, confidentiality

12. Subject Access Request (SAR)

Individuals are entitled to a copy of their personal data upon request. The school is obliged to confirm the identity of any person making such a request. ***(See Appendix 7 for the Data Subject Request Form).*** The period for response is 30 calendar days but this period may be extended by two further months in cases where the request is particularly complex, or where multiple requests have been received at the same time. No fee may be charged except in exceptional circumstances where the requests are repetitive or manifestly unfounded or excessive.

The individual's access to their personal data is subject to some exemptions and prohibitions set down in the Data Protection Acts. No personal data can be supplied relating to another individual apart from the data subject. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

Although those students who are under 18 are regarded as minors under the law, they still have the right under the Data Protection Acts for information about them not to be disclosed without their consent.

13. Breaches of Policy:

A ***personal data breach*** may occur where the security or integrity of personal data is compromised. This can arise through misappropriation, loss or theft of data or equipment, unauthorised individuals gaining access, a deliberate attack on systems, equipment failure, human error or malicious acts such as hacking, viruses or deception. Any staff member that suspects that a data breach may have occurred, must notify the principal immediately. If the breach is substantiated and where the breach presents a risk to the affected individual, the Principal, on behalf of the Board of Management, has a mandatory obligation to notify the office of the ***Data Protection Commissioner*** within 72 hours. Where the breach is likely to result in a high risk to the affected individual, the BoM must communicate the personal data breach to the data subject without undue delay.

14. Review and Evaluation:

This policy is subject to review and evaluation on a biannual basis. Cognisance of changing information, guidelines, legislation and feedback from parents/guardians, students, school staff and others may necessitate amendments to the policy within a shorter time frame.

15. Implementation and Ratification:

This policy was first adopted on the 27th of May 2019.

Mr. Frank Gallen,
Chairperson of Board of Management

Fr. Éanna ÓhÓbáin O.Carm.,
Principal

The next date for ratification is due May 2021.

Appendix 1 **Glossary of Key Terms**

The ***Data Controller*** is a person, company or other body that determines the purpose and means of personal data processing. In the context of a school, the data controller is the Board of Management of the school.

Data Processing means any operation or set of operations which is performed on personal data, including the collection, recording, organisation, structuring, storage, alteration, use of, retrieval, disclosure or transmission of information.

The ***Data Processor*** is a person or service provider who processes personal information on behalf of a data controller.

The ***Data Protection Acts*** refer to the Data Protection Acts 1988 to 2018.

The ***Data Protection Commissioner*** is the independent national authority responsible for upholding the EU fundamental right of individuals to data privacy through the enforcement and monitoring of compliance with data protection legislation in Ireland.

Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28

Phone: 0761-104800

The ***Data Subject*** is an individual who is the subject of personal data.

Personal Data is any data relating to an identified or identifiable living person.

A ***Personal Data Breach*** is 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.

A ***Privacy by Design*** method promotes the concept that any action an organisation undertakes that involves processing personal data must be done with data protection and privacy in mind at every step.

A Subject Access Request (SAR): A Subject Access Request (SAR) entitles individuals to obtain a copy of their personal data, as well as other supplementary information.

Appendix 2 **Students**

Data	Why/Purpose	Shared With	Format & Security	Time Held	Disposal
Rollbook/School Register Personal Details Timetable Data School Reports Data & Results Attendance Behaviour Psychological Educational Reports & Special Educational Needs Information e.g. SEN Reports & Testing ECA Involvement Garda Vetting where relevant (TY) Medical Details Pastoral Care e.g. Chaplaincy, Guidance Counsellor, Matron Permission Forms Form Masters Diaries & Notebooks Bullying Reports Incident Reports Child Protection Records Username & Password for VSWare Photographic & Video Images College Publications e.g. Newsletters, Annual etc.	To comply with legislative and administrative requirements. To ensure that eligible students can benefit from relevant additional teaching/financial supports and to facilitate students eligible for language exemptions. To enable parents/guardians to be contacted in the case of emergency or school closure and to inform them of their child's educational progress. To facilitate the enrolment process. To furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, etc, and other schools in compliance with law and directions issued by government departments. Historical and archive purposes.	Relevant college personnel. Third parties, including other government bodies. This includes the State Examination Commission, the Department of Education and Skills, the National Council for Special Education, Tusla, An Garda Siochána, etc.	Individual student data is kept in secure storage units in designated areas including administrative and management offices. Digital data is kept password secured and all work devices are encrypted. Data is stored and managed using VSware – a design led, cloud and mobile based school administrative platform.	18 years of age plus seven years. Hold indefinitely data which relates to issues of child protection, mental health assessments, accident reports, school trips or filing of serious complaints. Exam results can be held for longer than stated if the data is pseudonymised to protect the subject's identity.	Confidential shredding and/or deletion on database.

Note: The school attendance record should be held indefinitely. Teacher rollbooks should be only retained for the duration for which the teacher educates the students. Relevant grades and other information pertaining to students should be passed onto the form master and/or subsequent teachers.

Appendix 3 **Parents/Guardians**

Data	Why/Purpose	Shared With	Format & Security	Time Held	Disposal
Bank Details	For payment of fees	Relevant college personnel.			Confidential shredding after payment transaction has been processed.
Personal Details Fee Payment Record Username & Password for VSWare Correspondence/Communications Meeting Notes Child Protection Records	For administrative purposes. To enable correspondence between the school and parents/guardians. To communicate events and activities that relate to the college and wider community.	Relevant college personnel. Third parties, including other government bodies. This includes the Department of Education and Skills, Tusla, An Garda Siochána, etc.	Digital data is kept password secured and all work devices are encrypted. Data is stored and managed using VSware – a design led, cloud and mobile based school administrative platform.	18 years of age plus seven years. Hold indefinitely data which relates to issues of child protection or filing of serious complaints.	Confidential shredding and/or deletion on database.

Appendix 4 **Staff**

Data	Why/Purpose	Shared With	Format & Security	Time Held	Disposal
Personal Details Curriculum Vita Letters of Application References Contracts Teaching Post Details Qualifications Bank Details Garda Vetting Code of Behaviour for Workers Username for VSWare Timetables Substitution Records Medical Documentation e.g. Certificates, Medmark etc. Correspondence Notes of Meetings/Proceedings etc Attendance Training Interview Notes & Application Forms Leave Forms Teaching Council Registration Details Payroll Statutory Declaration & Form of Undertaking. Tusla Certs for CP Training	For administrative and human resource purposes, and the general management of the school. To facilitate the payment of staff, and to calculate other benefits/ entitlements/ pension payments/redundancy payments To record promotions and changes in responsibilities. To enable the school to comply with its obligations as an employer. To enable the school to comply with the requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies. Historical and archive purposes.	Relevant college personnel. Third parties, including other government bodies. This includes the Department of Education and Skills, An Garda Siochána, etc.	Individual staff data is kept in secure storage units in designated areas including administrative and management offices. Digital data is kept password secured and all work devices are encrypted.	Retain for duration of employment plus seven years. Hold indefinitely data which relates to issues of child protection or filing of serious complaints.	Confidential shredding and/or deletion on database.

Appendix 5 **External Groups/Service Providers**

Data	Why/Purpose	Shared With	Format & Security	Time Held	Disposal
Contact Person's Name Contact Person's Telephone Contact Person's Email Groups Postal Address Confirmation of Group's Child Protection Policy Group's Insurance Policy Details Bank/Financial Details	To record details of external groups who use the college facilities. To record details of service providers who facilitate in the daily running and upkeep of the school. To meet statutory legal requirements. To enable correspondence between the school and the external groups/service providers.	Relevant college personnel. Relevant government bodies as required.	Data is kept in secure storage units in designated areas including administrative offices.	Retain for one year after last correspondence. Hold indefinitely data which relates to issues of child protection or filing of serious complaints.	Confidential shredding and/or deletion on database.
Payroll & Taxation	To facilitate payment and taxation.		Digital data is kept password secured and all work devices are encrypted.	Revenue require a seven year period after the end of the tax year.	
Invoices & Receipts	To monitor cashflow. To keep financial records to assist in any auditing process.				
Audited Accounts	To facilitate mandatory audits.			Hold indefinitely.	
Board of Management Records	To enable the board of management to carry out its duties and responsibilities.				

Appendix 6 **Job Applicants**

Data	Why/Purpose	Shared With	Format & Security	Time Held	Disposal
Curriculum Vitae Letters of Application References Garda Vetting Correspondence Interview Notes and Application Forms Teaching Council Registration Details Qualification Details	To facilitate the job application process.	Relevant college personnel. Interview board.	Job application data is kept in secure filling cabinets in designated storage areas including administrative offices. Digital data is kept password secured and all work devices are encrypted.	Retain for two years from close of competition. Retain unsolicited applications for six months.	Confidential shredding and/or deletion on database.

Request Form

Name of Applicant	
Address	
Contact Number	
Contact Email	
Description of the information requested	
Are you the Data Subject?	Please tick: Yes: _____ No: _____
If **Yes** is ticked, please supply evidence of your identity, such as a birth cert, driving licence or passport.	
If **No** is ticked, please complete the remaining sections.	
Name of Data Subject	
Relationship to Data Subject	
Note that written authorisation from the data subject to act on their behalf must be provided (where applicable).	

DECLARATION – To be completed by all applicants.

Please note that any attempt to mislead may result in prosecution

I …….. certify that the information given on this application form to Terenure College is true. I understand that it is necessary for the school to confirm my/the data subject's identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signature: ……..

Date: ……