



Dominican College Griffith Avenue

Catholic Secondary School
For Girls Est 1883
Charity No. 2 01 4 5 6 6 8



Data Protection Policy

Reader Information	Title: Data Protection Policy
Purpose:	To outline the approved Dominican College's management approach to be followed in relation to Data Protection Policy.
Publication date:	1st November 2025
Target Audience:	All BOM, staff, service providers, students, parents, guardians and third parties that have access to the Dominican College information.
Superseded Documents:	All other Data Protection policies.
Review Date:	1st November 2026

1. Introduction

1.1 Background to the General Data Protection Regulation ('GDPR') and the Irish Data Protection Act 2018.

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever relevant, that it is processed with their consent.

The Irish Data Protection Act 2018 came into force on the 24th and 25th May 2018 with the exception of Sections 7(3), 25, 30, and 176(b). The Data Protection Act 2018 was enacted to Establish the Data Protection Commission and to give further effect to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and to repeal Directive 95/46/EC (*General Data Protection Regulation*); To give effect to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and to repeal the Council Framework Decision 2008/977/JHA; (*Directive*); To give further effect to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January 1981; To amend the Data Protection Act 1988; to provide for the consequential amendment of certain other enactments; and to provide for related matters.

The school is also cognisant of other legislation which relates to the processing of personal data, whether in manual or in electronic form, such as the e-Privacy Regulations which provide statutory guidance with regard to certain data processing operations (e.g. direct marketing, cookie notifications on school website etc.).

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. These responsibilities also stem from a desire to process all personal data in an ethical manner which respects and protects the fundamental rights and freedoms of natural persons (students, parents / guardians and staff and others).

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 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).

Amendments to this Data Protection Policy or any change to the purpose of processing personal data 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.

1.2 Material and Territorial Scope of the GDPR

‘GDPR Material scope’ (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system, or which are intended to form part of a filing system.

‘GDPR Territorial scope’ (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It also applies to controllers outside of the EU that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the EU.

The school accepts the obligation and requirements imposed by the General Data Protection Regulations in respect of its processing of data and has implemented policies and procedures to protect personal data.

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 shared¹.

1.3 Definitions (Article 4)

‘Establishment’ – the main establishment of the ‘Controller’ in the European Union will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a ‘Processor’ in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a ‘Representative’ in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

‘Personal data’ – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

‘Special categories of personal data’ – personal data 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.

‘Data controller’ – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

‘Data subject’ – any living individual who is the subject of personal data held by an organisation.

‘Processing’ – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use,

¹ JMB's Template Data Protection Policy April 2019.

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. (Processing can include any activity that might relate to personal data under the control of the school, including the storage of personal data, regardless of whether the records are processed by automated or manual means).

‘Profiling’ – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

‘Personal data breach’ – 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. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject to the data subject.

‘Data subject consent’ - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

‘Child’ – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The controller shall make reasonable efforts to verify in such cases that consent when required is given or authorised by the holder of parental responsibility over the child².

‘Third party’ – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

‘Filing system’ – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

‘Data Protection Commission’ - the national supervisory authority responsible for monitoring the enforcing the data protection legislation within Ireland. The DPC is the organisation to which schools as data controllers must notify data breaches where there is risk involved.

2. Policy statement

² Recital 38 GDPR the consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

2.1 Dominican College located at 204 Griffith Ave, Dublin 9. D09A5XO is committed to compliance with all relevant European Union and Member State laws in respect of personal data, and the protection of the “rights and freedoms” of individuals whose information Dominican College collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2 Compliance with the GDPR is described by this policy and other relevant policies implemented by Dominican College together with the related mechanisms, processes and procedures as required by the GDPR and Data Protection Acts.

2.3 The GDPR, Data Protection Acts and this policy apply to all Dominican College’s personal data processing functions performed on students, parents / guardians, staff, board of management and trustees’ personal data, and any other personal data that Dominican College may process from other source(s).

2.4 Dominican College has established requirements for the protection and privacy of personal data, which are outlined in Dominican College’s policies, processes, mechanisms and procedures.

2.5 Dominican College is responsible for annually reviewing the GDPR register of processing, as well as any review that may be required in the event of any changes to Dominican College’s activities (as determined by changes to the mapping of life cycle of personal data / the management’s review(s)) as well as to any additional requirements identified by means of Data Protection Impact Assessment.

2.6 This policy applies to all Dominican College’s staff. Any breach of the GDPR will be dealt with by Dominican College’s and may also be a criminal offence, in which case the matter will be reported, as soon as possible to the appropriate authorities.

2.7 Any person working with or for Dominican College and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

2.8 No authorised third party may access personal data held by Dominican College without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which Dominican College is committed, and which gives Dominican College the right to audit compliance with the agreement.

3. Responsibilities and roles under the General Data Protection Regulation

3.1 Dominican College is a data controller and/or data processor under the GDPR.

3.2 The Management and all those in managerial or supervisory roles throughout Dominican College are responsible for developing and encouraging good information handling practices within Dominican College.

3.3 The Principal being a member of the senior management team, is accountable to Dominican College for the management of personal data within Dominican College and for ensuring that compliance with data protection legislation and good practice is demonstrated. This accountability includes:

3.3.1 development and implementation of the GDPR as required by implemented policies and

3.3.2 security and risk management in relation to compliance with implemented policies.

3.4 The Principal has been appointed to take responsibility for Dominican College compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Dominican College complies with the GDPR, as do other managers in respect of all data processing that takes place within their area of responsibility.

3.5 The Principal has specific responsibilities in respect of procedures such as the Subject Access Request Procedure etc. and is the first point of call for staff members seeking clarification on any aspect of data protection compliance.

3.6 Compliance with data protection legislation is the responsibility of all staff of Dominican College who process or are involved in the processing of personal data.

3.7 Dominican College's Training Policy sets out specific training and awareness requirements in relation to staff of Dominican College.

3.8 Staff of Dominican College are responsible for ensuring that any personal data about them and supplied by them to Dominican College is accurate and up to date.

3.9 Staff of Dominican College must be made aware of and comply with the relevant technical or organisational measures implemented to ensure a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the data concerned.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR (fair, lawful, transparent, specific purpose, adequate, limited, accurate, retained for no longer than is necessary, with appropriate integrity & confidentiality). Dominican College's policies and procedures are designed to ensure compliance with these principles. 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.

4.1 Personal data must be processed lawfully, fairly and transparently (**lawfulness, fairness and transparency**)

‘Lawful’ – identify a lawful basis before you can process personal data. These are often referred to as the “conditions for processing”, for example consent, contract, legal obligation, vital interests, public interest, legitimate interests.

‘Fairly’ – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources. The GDPR has increased requirements about information that should be made available to data subjects, in the ‘Privacy Notice’.

‘Transparently’ – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. It also requires that information must also be communicated to the data subject in an intelligible form using clear and plain language.

‘Privacy Notice’

Dominican College’s Privacy Notice is set out on its website <https://dominican-college.com/>
The specific information that must be provided to the data subject as a minimum, includes:

4.1.1 the identity and the contact details of the controller and, if any, of the controller's representative.

4.1.2 the contact details of the GDPR Controller.

4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing as well as the obligation to provide personal data.

4.1.4 details of the sharing of personal data.

4.1.5 the period for which the personal data will be stored.

4.1.6 product and service-related data

4.1.7 the existence of the rights to request access, rectification, erasure restriction, portability or to object to the processing, withdrawal of consent, to lodge a complaint and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected.

4.1.8 security of personal data

4.1.9 risks and safeguards

4.1.10 rules in relation to the processing of personal data

4.1.11 the categories of personal data concerned.

4.1.12 the recipients or categories of recipients of the personal data, where applicable.

4.1.13 that the controller intention to transfer personal data to a recipient in a third country and the level of protection afforded to the transfer of such data.

4.1.14 any further information necessary to guarantee fair processing.

4.1.15 contact details of Dominican College

4.1.16 provision of the contents of the Privacy Notice orally

4.1.17 effects on personal data from browsing, and the use of cookies the website of Dominican College at <https://dominican-college.com/>

4.1.18 automatic Decision Making (Profiling)

4.1.19 account management, market research or surveys

4.1.20 e-mail communications policy

4.1.21 links

4.1.22 notification of changes

4.2 Personal data can only be collected for specific, explicit and lawful purposes (**Purpose Limitation**). Personal data obtained for specified purposes must not be used for a purpose that differs from those that applied and were specified in the Privacy Notice at the time of collection of the personal data.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing (**Data Minimisation**).

4.3.1 The Controller is responsible for ensuring that Dominican College does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in the case of new information systems, will include a fair processing statement or link to the Privacy Notice and be approved by the Controller.

4.3.3 The Controller will ensure that, on an annual basis, all data collection methods are reviewed to ensure that the collected data continues to be adequate, relevant and not excessive (Data Protection Impact Assessment procedure will be utilised as required).

4.4. Personal data must be accurate and kept up to date and erased or rectified without delay, where it is found to be inaccurate. (**Accuracy**)

4.4.1 Data that is stored by the data controller must be reviewed and updated, as necessary. No inaccurate data should be retained unless efforts are in motion to have it rectified.

4.4.2 The GDPR controller is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of Dominican College to request data subject to ensure that data held by Dominican College is accurate and up to date. Data subjects when completing any registration, application or other form should ensure that the data supplied is accurate at the date of submission.

4.4.4 Staff/Students/Parents/Guardians or others should notify Dominican College of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Dominican College to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.5 The Controller is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.6 On an annual basis, the Controller will review the retention dates of all the personal data processed by Dominican College by reference to the data inventory and will identify any personal data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Disposal and Destruction Policy.

4.4.7 The Controller is responsible for responding to requests of rectification from data subjects within one month (Subject Access Request Procedure). This can be extended to a further two months for complex requests, but the data subject must be informed of the delay and reasons for any such delay within 30 days of receipt of their application. If Dominican College decides not to comply with the request, the Controller will respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and / or seek judicial remedy.

4.4.8 The Controller is responsible for making appropriate arrangements, where third-party organisations may have been passed inaccurate or out-of-date personal

data, to inform the third party that the information is inaccurate and/or out of date and that it should not be used to inform decisions about the individuals concerned; as well as passing any correction to the personal data to the third party where this is relevant.

4.5 Personal data must be kept in a form such that the data subject can be identified for only as long as is necessary for its processing.

4.5.1 Personal data processed, will be minimised, and encrypted where possible when stored in order to protect the identity of the data subject in the event of a data breach.

4.5.2 Personal data will be retained in line with the Personal Data Retention Policy and, once its retention date is reached, its purpose of retention must be assessed and either have its expiry date amended or else have it securely destroyed or deleted (**Storage Limitation**).

4.5.3 The GDPR Controller will specifically approve any data retention that exceeds the retention periods defined in Personal Data Retention Policy and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval will be in writing.

4.5.4 Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

The Controller will carry out a risk assessment taking into account all the circumstances of Dominican College controlling or processing operations.

In determining appropriateness, the GDPR controller will also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or students, parents / guardians) and if a security breach occurs, the effect of any security breach on Dominican College itself, and any likely reputational damage including the possible loss of students, parents / guardians trust.

4.5 The controller must be able to demonstrate compliance with the GDPR's other principles (**accountability**). The GDPR includes provisions that promote accountability and governance to complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires demonstration with these principles. Dominican College demonstrates compliance with the data protection principles by implementing data protection notice, policies, implementing technical and organisational measures / mechanisms, as well as implementing data protection by design and default, Data Protection Impact Assessments, and Data Breach Notification Policy.

4.6 The appropriate technical and organisational measures implemented for the protection of personal data shall be reviewed yearly unless they required to be reviewed sooner.

5. Lawful Basis for Processing Personal Data

Whenever Dominican College is processing personal data, all of the principles listed above must be obeyed. In addition, at least one of the following lawful bases for processing personal data as required under Article 6 of the GDPR must apply if the processing is to be lawful,

- I. consent,
- II. contract,
- III. in compliance with a legal obligation,
- IV. vital interests of the data subject,
- V. necessary in the public interest,
- VI. legitimate interests of the controller

When processing special category personal data, Dominican College will ensure that it has additionally identified an appropriate lawful basis under GDPR Article 9 in relation to Special categories of personal data such as 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.

6. Data subjects' rights

6.1 The data subject rights are addressed through the school's privacy notice, policy on data subject's rights, data protection policy, and replying to any questions or queries submitted by data subjects.

Data subjects have a right to the

- protection of their personal data,
- right to information
- right to access their personal data,
- right to rectification of their personal data,
- right to erasure of their personal data in certain circumstances,
- to be notified,
- to be forgotten,
- to restriction,
- to portability,
- to objection,
- to withdraw their consent (where applicable),
- to reject automated individual decision making in certain circumstances
- to make a complaint,

It is important to note that data subject's rights are not without limitations, while the school will always facilitate the exercise of data subject's rights, it may need to give consideration to other obligations when addressing data subject's rights.

Data subjects have the following rights regarding data processing, such as the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and in relation to any personal data being recorded the following rights.

6.1.1 To make a subject access request regarding the nature of information held and to whom it has been disclosed.

6.1.2 To prevent processing likely to cause damage or distress.

6.1.3 To prevent processing for purposes of direct marketing without consent.

6.1.4 To be informed about the mechanics of any automated decision-taking process that will significantly affect them.

6.1.5 To not have significant decisions that will affect them taken solely by automated process.

6.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

6.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

6.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

6.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

6.1.10 To object to any automated profiling that is occurring without consent.

6.2 Dominican College ensures that data subjects may exercise these rights:

6.2.1 Data subjects may make data access requests as described in Data Subjects Rights Policy and Dominican College will ensure that its response to the data access request complies with the requirements of the GDPR.

6.2.2 Data subjects have the right to complain to Dominican College in relation to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the complaint's procedure.

7. Recipients

Recipients of personal data are defined as organisations and individuals to whom Dominican College transfers or discloses personal data. Recipients may be data controllers, joint controllers or processors. A list of the categories of recipients to whom personal data may be shared with provided in the appendices (Appendix 'A'). This list may be subject to change from time to time and on a case-by-case basis.

8. Data Sharing Guidelines

- 8.1 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 e.g. the Gardaí may submit a valid request under the Irish Data Protection Act to process necessary and proportionate for the purposes of preventing, detecting, investigating or prosecuting criminal offences.
- 8.2 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.
- 8.3 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 and Skills. As such their actions will be governed by national and European data protection legislation as well their own organisational policies³.
- 8.4 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.

9. Consent

9.1 Dominican College understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. A data subject can withdraw their consent at any time.

9.2 Dominican College understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement and that consent obtained under duress or on the basis of misleading information will not be a valid basis for processing of personal data.

9.3 Dominican College also acknowledges that there must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate where applicable that consent was obtained for the processing operation.

³ The Data Protection Policy of the Department of Education and Skills can be viewed on its website (www.education.ie)

9.4 In the case of sensitive data, explicit written consent of data subjects is required to be obtained unless an alternative legitimate basis for processing exists.

9.5 In most instances, the legal basis for processing personal is based on legal obligation on the part of Dominican College using standard documents.

10. Security of data

10.1 All staff are responsible for ensuring that all personal data that Dominican College holds and for which they are responsible, is kept securely and is not disclosed under any conditions to any third party unless that third party has been specifically authorised by Dominican College, and subject to the data subject's consent to the sharing of personal data, (Where applicable) as well as the third party having entered into a contract / confidentiality agreement as required by GDPR and Data Protection Acts.

10.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Data Security Policy. All personal data should be treated with the highest security and must be kept:

- in a secure location with controlled access; and/or
- in a secure drawer or filing cabinet or other secure location; and/or
- if computerised, password protected in line with business requirements in the Data Security Policy: and/or
- stored on (removable) computer media and encrypted (where possible) in line with Disposal and Destruction Policy.

10.3 Care must be taken to ensure that computer screens and terminals are not visible except to authorised employees/staff of Dominican College. All staff are required to enter into a Confidentiality Agreement before they are given access to organisational information of any sort, and in particularly in relation to personal data.

10.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed and secured in line with personal data retention policy.

10.5 Personal data may only be deleted or disposed of in line with the Disposal and Destruction Policy. Manual records that have reached their retention expiry date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and destroyed where they cannot be reformatted in accordance with the instructions of the Principal before disposal.

10.6 In order to determine the "Appropriate Technical & Organisational Measures" required to be implemented, the controller or processor shall where relevant have regards to the following

- a. the nature of the personal data concerned.

- b. the accessibility of the data.
- c. the nature, scope, context and purpose of the processing concerned.
- d. any risks to the rights and freedoms of individuals arising from the processing.
Concerned.
- e. the likelihood of any such risks arising and the severity of such risks.
- f. the state of the art and the cost of implementation.
- g. guidelines, recommendations and descriptions of best practice issued by the
Commission or the European Data Protection Board.

11. Disclosure of data

11.1 Dominican College must ensure that personal data is not disclosed to unauthorised third parties. All staff are required to exercise caution when asked to disclose personal data held on data subjects to a third party.

11.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Controller.

12. Retention and disposal of data

12.1 Dominican College shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary in relation to the purpose(s) for which the data was originally collected and processed.

12.2 Dominican College may store data for longer periods if the personal data is to be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

12.3 The retention period for each category of personal data will be set out in the Personal Data Retention Policy along with the criteria used to determine this period, including any statutory obligations that Dominican College has to adhere to in relation to the retention of the personal data.

12.4 Dominican College's personal data retention policy and Disposal and Destruction Policy applies in all cases.

12.5 Personal data must be disposed of securely in accordance with the principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the

“rights and freedoms” of data subjects. Any disposal of data will be done in accordance with the Disposal and Destruction Policy.

13. Processor

Where processing of personal data is processed by a processor on behalf of the Controller, a contract or other legal act, in writing between both parties is required and shall contain such details as are shown hereunder.

- a. Specify the subject matter, duration, nature and purpose of the processing to be carried out thereunder,
 - b. Specify the type of personal data to be processed thereunder and the categories of data subjects to whom the personal data relate,
 - c. Specify the obligations and rights of the Controller in relation to the processing,
- and
- d. provide that the processor shall:
 - i. act only on instructions from the Controller in relation to the processing, except in so far as the law of the European Union or the law of the State requires the processor to act otherwise,
 - ii. procure the services of another processor (in this section referred to as a “secondary processor”) in relation to the processing only where authorised to do so in advance and in writing by the Controller, which authorisation may be specific or general in nature,
 - iii. ensure that any person authorised to process the personal data has undertaken to maintain the confidentiality of the personal data or is under an appropriate statutory obligation to do so,
 - iv. assist the Controller in ensuring compliance with the exercise by a data subject of his or her rights,
 - v. erase or return to the Controller, at the election of the Controller, all personal data upon completion of the processing services carried out by the processor on behalf of the Controller and erase any copy of the data, unless the processor is required by the law of the European Union or the law of the State to retain the data, and
 - vi. make available to the Controller all information necessary to demonstrate compliance by the processor with this section.

•

14. Data transfers

14.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as ‘third countries’) are unlawful unless there is an appropriate “level of protection for the fundamental rights of the data subjects”. The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

14.1.1 An adequacy decision - The European Commission can assess any third countries, territory and/or specific sectors within third countries in order to assess whether or not

there is an appropriate level of protection for the rights and freedoms of natural persons. In such instances no authorisation is required in relation to Countries that are members of the European Economic Area (EEA) including other third countries or international organisations that are accepted as having met the conditions for an adequacy decision. A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union*.

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

14.1.2 An assessment of adequacy requires an assessment of the adequacy of protection afforded to data subjects in relation to the processing of their data by the third country when considering exporting of personal data there.

The following factors are required to be taken into account:

- the nature of the information being transferred.
- the country or territory of the origin, and final destination of the information
- how the information will be used and for how long
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations and
- the security measures that are to be taken as regards the data in the overseas location.

14.1.3 Binding corporate rules - Dominican College may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant supervisory authority for approval of the rules that Dominican College would be seeking to rely upon.

14.1.4 Model contract clauses - Dominican College may adopt approved model contract clauses for the transfer of data outside of the EEA if applicable.

14.1.5 Exceptions - In the absence of an adequacy decision, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject to the absence of an adequacy decision and appropriate safeguards.
- the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken at the data subject's request.
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- the transfer is necessary for important reasons of public interest.
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or

- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

15. Information asset register/data inventory

15.1 Dominican College has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project.

Dominican College data inventory and data flow determine.

- School processes that use personal data
- source of personal data
- description of each item of personal data
- processing activity
- maintains the inventory of data categories of personal data processed.
- documents the purpose(s) for which each category of personal data is used.
- recipients, and potential recipients, of the personal data
- the role of Dominican College throughout the data flow
- key systems and repositories
- any data transfers; and
- all retention and disposal requirements.

15.2 Dominican College need to be aware of any risks associated with the processing of particular types of personal data.

15.2.1 Dominican College has assessed the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) have been conducted in relation to the processing of personal data by Dominican College, and in relation to any processing undertaken by other organisations on behalf of Dominican College.

15.2.2 Dominican College is managing identified risks through the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

15.2.3 Where a type of processing is being undertaken, in particular when using new technologies, the controller shall take into account the nature, scope, context and purposes of the processing where it is likely to result in a high risk to the rights and freedoms of natural persons, Dominican College shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

15.2.4 Where, as a result of a DPIA it is clear that Dominican College is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Dominican College may proceed must be escalated for review to the GDPR Controller.

15.2.5 The GDPR Controller shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

15.2.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data as required by the GDPR and Data Protection Acts.

16. Other Legal Obligations

Implementation of this policy takes cognisance of the school's other legal obligations and responsibilities. Some of these are directly relevant to data protection as outlined hereunder.

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education.
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the school.
- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring.
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day.
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply Personal Data kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)
- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers

("SENOS")) such information as the Council may from time-to-time reasonably request.

- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body.
- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection.
- Under Children First: National Guidance for the Protection and Welfare of Children (2011) published by the Department of Children & Youth Affairs, schools, their Boards of Management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

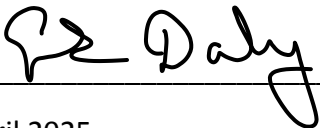
17. Data Controller

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

18. Compliance Monitoring and Review

Dominican College will undertake regular reviews of internal procedures and changes in the legislation to ensure ongoing compliance with General Data Protection Regulation. This will include an annual review.

Signed:  Chairperson, Board of Management

Date: 8th April 2025

Appendix “A”

Categories of Recipients of Personal Data Processed

Department of Education and Skills (DES) - the school is required to provide student data to the Department of Education and Skills (DES). This transfer of data is primarily made at the beginning of each academic year (“October Returns”) using a secure Post-Primary Online Database (P-POD) system. The October Returns contain individualised data such as PPS number which acts as an identifier to validate that the data belongs to a recognised student. The DES has published a “Fair Processing Notice” to explain how the personal data of students is processed⁴.

State Examinations Commission (SEC) - data on entrants for the state examinations is provided via the October Returns to SEC to assist its planning of the state examinations.

Student support and welfare - student data may be shared with a number of public state bodies including National Educational Psychological Service (NEPS psychologists support schools and students); National Council for Special Education (the NCSE role is to support schools and students with special education needs); National Education Welfare Board (the school is required to share student attendance with the NEWB). Data to support student access to further and higher education may also be shared for processing as part of Student Universal Support Ireland (SUSI), Higher Education Access Route (HEAR) and Disability Access Education Route (DARE).

Legal requirements - where appropriate, particularly in relation to Child Protection and safeguarding issues, the school may be obliged to seek advice and/or make referrals to Túsła⁵. The school may share personal data with An Garda Síochána where concerns arise in relation to child protection. The school will also report matters of alleged criminal acts, criminal behaviour, criminal damage, etc., to allow prevention, detection and investigation of offences. Where there is a lawful basis for doing so, personal data may also be shared with the Revenue Commissioners and the Workplace Relations Commission.

Insurance - data may be shared with the school’s insurers where this is appropriate and proportionate. The school may also be obliged to share personal data with the Health and Safety Authority, for example, where this is required as part of an accident investigation.

Professional Advisors - some data may be shared with legal advisors (solicitors, etc.), financial advisors (pension administrators, accountants, etc.) and others such as school

⁴ These can be found on www.education.ie (search for Circular Letters 0047/2010 and 0023/2016 in the “Circulars” section). The Department of Education and Skills transfers some student data to other government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection & Employment Affairs pursuant to the Social Welfare Acts, transfers to the State Examinations Commission, transfers to the Educational Research Centre, and transfers to the Central Statistics Office pursuant to the Statistics Acts. The data will also be used by the DES for statistical, policymaking and research purposes. However, the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes.

⁵ Túsła, the Child and Family Agency, is the State agency responsible for improving wellbeing and outcomes for children.

management advisors; this processing will only take place where it is considered appropriate, necessary and lawful.

Other schools and Universities/Colleges/Institutes - where the student transfers to another educational body, or goes on an exchange programme or similar, the school may be asked to supply certain information about the student, such as academic record, references, etc.

Work Placement - some data may be shared, on request, with work placement providers and employers where this is appropriate and necessary to support students engaged in work experience or similar programmes.

Voluntary Bodies - some personal data may be shared as appropriate with bodies such as the school's Parents Association. This data sharing will only take place where consent has been provided.

Other not-for-profit organisations - limited data may be shared with recognised bodies who act to promote student engagement with co-curricular and other activities, competitions, recognition of achievements, etc. This would include bodies promoting participation in sports, arts, sciences, environmental and outdoor activities, etc. This data sharing will usually be based on consent.

Service Providers - in some circumstances the school has appointed third parties to undertake processing activities on its behalf. These Data Processors have provided guarantees that their processing satisfies the requirements of the General Data Protection Regulation. The school has implemented written contractual agreements with these entities to ensure that the rights of data subjects receive an appropriate level of protection. Third party service providers include the following categories:

- School Management Information Systems – (e.g. VSware)
- Productivity Applications (e.g. Google Apps for Education, Microsoft 365)
- Online Storage & File Sharing (e.g. Dropbox, Google Drive, iCloud, OneDrive)
- Video Sharing and Blogging Platforms – (e.g. YouTube, Facebook)
- Virtual Learning Environments – (e.g. Google Classroom)
- IT Systems Support
- Fee management software
- School communications – (e.g. Unique Publishing)
- Security and CCTV Systems
- Pension Consultants/Trustees
- Accounting & Payroll software
- Cashless Payment Systems
- Canteen Management System
- Learning software and Apps

Transfers Abroad - In the event that personal data may be transferred outside the European Economic Area (EEA) the school will ensure that any such transfer, and any subsequent

processing, is carried out in strict compliance with recognised safeguards or derogations (i.e., those approved by the Irish Data Protection Commission).

Appendix “B”

Personal Data and Related Processing Purposes

Purpose for Processing	Description of Personal Data
1. Contact and identification information. This information is needed to identify, contact and enrol students.	
Purposes may include: • to add names to a contact list prior to formal application • to provide appropriate information to prospective students • to make contact in case of school closure (e.g. adverse weather conditions). • to send SMS text messages and emails about meetings, etc.	Information required to confirm student/parent identity and contact through communications: • student name. • gender • date of birth • family details (parents/guardians name, address, contact details to include phone numbers, email addresses etc).
2. Application information We use this to determine whether an applicant meets eligibility requirements as set out in our Admission Policy.	
In addition to data outlined at (1) above, we collect personal data via Application Forms and Student Transfer Forms. Where the student is offered a place, completed Application Forms are placed on the student’s file. Where the student is not offered a place, the data will be used for the purposes of responding to any section 29 appeals process. Applicants may opt to provide data on “Religion” at this stage where this forms part of the school’s admissions criteria. Any information not required to operate the Admissions Procedure, is identified as optional.	Information as required to ascertain eligibility under the school’s Admissions Policy: • Name and address of current school • Class in current school • Details of siblings, etc. • Details of any special educational needs (SEN). (NB only for admission to a special school, or a SEN unit). • Language: details re Irish language. • Religion
3. Enrolment information Once the school has accepted the student’s application, and has offered the student a place, other information is collected in addition to the data outlined at (1) and (2) above. This personal data is used for administrative and management tasks e.g. school communications, timetabling, scheduling parent teacher meetings, school events, arrangements for academic registration, class details, start dates, book lists, subject-selection, school trips etc.	

<u>Contact and Identification Information:</u> We use this information: • to make contact in case of school closure (e.g. adverse weather conditions), or an emergency (ill-health or injury), • to communicate issues relating to progress, welfare or conduct in school, non-attendance or late attendance, etc. • to send SMS text messages and emails about important events, e.g. start dates, course details, meetings, school events, etc.	• Student name and date of birth (requires birth certificate verification by school) • PPSN, Address including Eircode • Extended family details (parent/guardian names, contact details, postal & email address, phone numbers, addresses, details of any court orders or other arrangements governing access to, or custody of, child (if applicable). • Details of next of kin (for contact in case of emergency)
<u>Academic record:</u> We use this information to deliver education appropriate to the needs of the student, to assess the student's educational progress. Standardised test results used for the purposes of assessing literacy/numeracy progress, for Reasonable Accommodation in State Examinations, for assisting in referrals to NEPS, and for career guidance etc.	• Reports, references, assessments and other records from any previous school(s) attended by the student. • Education Passport (6th Class Report provided by primary school after post-primary school confirms enrolment. Protocols set out in DES Circulars 42/2015 and 34/2016). • Standardised testing Results
<u>Language spoken:</u> Without this information the school will not know how to meet the student's needs and to deliver appropriate education. This ensures the student has access to language support (where necessary). <u>Irish Exemption</u> Information re application for Irish exemption if eligible (e.g. received primary school up to 11 years of age outside Ireland, evidence of disability, student from abroad etc).	• Information about language spoken (for language support) • Details of whether the student received EAL (English as an Additional Language) support. • Details re whether student is exempt from studying Irish • Details to ascertain if student is eligible for exemption from study of Irish
<u>Medical information for health purposes:</u> This information is essential to meet our duty of care to the student. We use this information to (i) ensure we know who to contact in case of emergency, (ii) ensure that we have relevant information to safeguard/prevent damage to student health (iii) meet medical/ care needs when students are in school (iv) facilitate appropriate advanced planning with parents/guardians (e.g. notification to relevant personnel within the school, storage of medications, staff training where necessary etc).	• Emergency contact details (name, telephone, details of relationship to the student etc). • Details of the student's GP (to be contacted in case of emergency). • Details of any relevant medical information (e.g. medical condition, allergies, treatment/care plan etc) to facilitate appropriate advanced planning with parents/guardians. This may include use of student's photograph for in cases of emergency action plan.

<u>SEN and Medical information for educational purposes:</u> We cannot meet our duty of care to the student and our obligations under EPSEN Act 2004 without this information. We use this information to (i) make application to the DES for allocation of resources to support student (ii) ensure school has relevant information to deliver education appropriate to student's needs (iii) apply for appropriate accommodation(s) and/or therapeutic supports where available.	• Details of any special needs/medical needs that need to be accommodated, e.g. medical assessment, hearing/ vision issues, psychological assessment/report. • Details of whether the student has been in receipt of learning support. • Details of whether the student been granted resource teaching hours and/or special needs assistance hours by the NCSE.
<u>Information sought by Department of Education and Skills (DES):</u> We are under a legal obligation to return specific enrolment information concerning each student to DES (SI 317/2015). This data is used to calculate teacher and resource allocation, capitation, grant payments for schools, for statistical analysis and reporting in the areas of social inclusion and integration of students in the education system, and for planning purposes. Other (optional) information is sought for purposes relating to planning, social inclusion and integration of students in the education system.	Personal data is transferred to the DES via the Post Primary Online Database as set out in the Privacy Notice for P-POD provided by DES. Required information includes, e.g. birth name of student and mother (to verify student identity). The DES seeks some additional information on an optional basis (i.e. based on parental consent), for example, • Ethnic/Cultural background
<u>Use of photographs for yearbooks, social media, website etc.:</u> Photographs, and recorded images of students may be taken at school events and to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school.	• Consent is sought to use (for these purposes) images or recordings in printed or digital format. • Separate consents will be sought if necessary for different publication forums. (NB This excludes CCTV recordings - see school CCTV policy).
<u>Religion</u> Religion is only sought where the school facilitates religious instruction/faith formation at the request of parent(s)/ guardian(s).	• Religious denomination (based on consent) or if it is chosen as a subject (legal basis)
<u>Consents to direct marketing:</u> If you wish to receive direct marketing, you can give consent for us to contact you by SMS text and/or email. Your right to opt-out only relates to the school contacting you for direct marketing purposes.	<u>Note:</u> We will still contact you on your mobile in case of an emergency relating to your child and/or to communicate messages about school events (e.g. school closure, parent teacher meetings etc).

4. Personal data gathered during student's time in School.

We cannot meet our statutory obligation to deliver appropriate education to students and/or we cannot satisfy our duty of care to each student without processing this information.

<u>Academic progress:</u> The school processes this personal data in order to deliver education to students, and to evaluate students' academic progress, to register the student for State Examinations (Junior Cycle, Leaving Cycle), to submit the students' work to the recognised accrediting body etc.	• Academic progress and results • State exam results • Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results) • Continuous assessment and end of term/year reports
<u>Attendance:</u> The school is required to collect and monitor attendance data and to notify the Education Welfare Officer (TUSLA) in certain circumstances, such as (i) where the student is suspended for 6 days or more (ii) where the student is absent for an aggregate period of 20 school days during the course of the year, (iii) where the Principal is of the opinion that the student is not attending school regularly. The school will notify parent/guardian in the event of non-attendance or absences.	Statutory processing pursuant to the Education (Welfare) Act 2000. • Attendance records including Registers and Roll books etc. • Records of referrals to TUSLA School Register and Roll Books are documents of enduring historical value and are retained in the school's archives for archival purposes in the public interest.
<u>School tours/trips:</u> Information required to make appropriate travel arrangements, to implement insurance cover, to arrange appropriate supervision ratios, to ensure medical/health issues are properly accommodated, to engage in responsible planning, and to ensure necessary paperwork for INIS (Irish Border Control/Irish Naturalisation & Immigration Service requirements where children are travelling with someone other than their parent or guardian).	Information to ensure trip is properly organised and supervised, including: • permission slips (signed by parents / guardians), • itinerary reports • Letter from parent(s)/guardian(s) giving consent to travel. • Copy of birth/adoption certificate or guardianship papers • Copy of marriage/divorce certificate (where parent has different surname to child). • Copy of the parent/guardian's passport or State identity document.
<u>Garda vetting outcomes:</u> Certain work experience roles may require that a student be Garda vetted (Statutory vetting process).	Information as set down in National Vetting Bureau (Children and Vulnerable Persons) Act 2012. • Garda vetting form
<u>CCTV images:</u> The school processes this data for the purposes outlined in our CCTV Policy, a copy of which is available on the school's website e.g. We use CCTV for	CCTV is in operation at the perimeter, exterior and certain internal common areas

security purposes; to protect premises and assets; to deter crime and anti-social behaviour; to assist in the investigation, detection, and prosecution of offences; to monitor areas in which cash and/or goods are handled; to deter bullying and/or harassment; to maintain good order and ensure the school's Code of Behaviour is respected; to provide a safe environment for all staff and students; for verification purposes and for dispute resolution, particularly in circumstances where there is a dispute as to facts and the recordings may be capable of resolving that dispute; for the taking and defence of litigation.	within the school both during the daytime and during the night hours each day. CCTV is used at external points on the premises (e.g. at front gates, in the carpark etc) and at certain internal points (e.g. front desk/ reception area, corridors etc). In areas where CCTV is in operation, appropriate notices will be displayed.
<u>Special needs data, educational support records, medical data etc:</u> Without this information, the school will not know what resources need to be put in place in order to meet the student's needs and to deliver appropriate education in-keeping with its statutory obligations. This is in order to assess student needs, determine whether resources can be obtained and/or made available to support those needs, and to develop individual education plans. Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (the statutory agency established under the Education for Persons with Special Educational Needs Act 2004) such information as the Council may from time-to-time reasonably request.	The school collects information relating to any special educational needs, psychological assessments/reports, information about resource teaching hours and/or special needs assistance hours, etc. Schools are also required to share this personal data with SENOs employed by the NCSE. • Psychological assessments, • Special Education Needs' files, reviews, correspondence • Individual Education Plans, • Learning support file, • Notes relating to inter-agency meetings, • Medical information (including details of any medical condition and/or medication / treatment required) • Psychological, psychiatric and/or medical assessments
<u>Child protection, child welfare records:</u> The school is required to follow DES Child Protection Procedures (Circular 81/2017) and to take appropriate action to safeguard the welfare of students in its care (Child Protection Procedures for Primary and Post-Primary Schools 2017). Staff have a legal responsibility to report actual or suspected child abuse or neglect to the Child & Family Agency ("TUSLA") and to An Garda Síochána. Mandatory reporting obligations arise under Children First 2015, the Criminal Justice (Withholding of	Mandatory reporting obligations require data sharing with TUSLA, An Garda Síochána and any other appropriate law enforcement or child protection authorities. DES Inspectorate may seek access to the school's child protection records for audit purposes. • Child protection records • Child safeguarding records • Other records relating to child welfare • Meitheal meetings convened by TUSLA

Information on Offences against Children and Vulnerable Persons) Act 2012.	
<u>Counselling & Pastoral Care Records:</u> This information is required to provide access to counselling services and/or psychological services and to provide supports to students, resolve behavioural, motivational, emotional and cognitive difficulties through assessment and therapeutic intervention, to engage in preventative work etc. Personal data (and special category personal data) will be shared with third parties (e.g. TUSLA, NEPS, CAMHS, An Garda Síochána, Medical practitioners treating the student) for the purpose of the school complying with its legal obligations and/or in the student's vital/ best interests.	• Guidance Counselling notes • Psychological service notes • Referrals to/records relating to therapeutic services and other interventions • Minutes, notes and other records concerning Student Support Team/Pastoral Care Team Meetings
<u>Internal school processes:</u> This information (e.g. anti-bullying processes and disciplinary/Code of Behaviour processes) is required to meet the school's duty of care to all its students and staff, to comply with relevant Circulars issued by the Department of Education and Skills, and to run the school safely and effectively. Data collected in these processes may be transferred to the school's insurer and/or legal advisors or management body as appropriate where required for disputes resolution, fact verification, and for litigation purposes.	• Records of parental complaints. • Records of other complaints (student to student complaints etc). • Records relating bullying investigations. • Records relating to Code of Behaviour processes (expulsion, suspension etc.) including appeals data and section 29 appeals material.
<u>Accident and injury reports:</u> This information is processed to operate a safe environment for students and staff, to identify and mitigate any potential risks, and to report incidents/ accidents. This data may be transferred to the school's insurance company and/or indemnifying body and/or legal advisors as appropriate. Data will be shared with An Garda Síochána, TUSLA and the Health & Safety Authority where appropriate.	• Accident reports • Incident Report Forms • Notifications to insurance company • Exchanges with legal advisors. • Notifications to Health & Safety Authority (HSA)
<u>Financial information, fees etc:</u> Without this information, the school cannot process applications, make grant payments, or receive payment of monies (e.g. course fees, school trips etc). After completion of the payments, the documentation is	• Information relating to payments from student's parents/ guardians (including fee support and fee waiver documentation), • Scholarship/Grant ap

retained for audit and verification purposes. The school's financial data are audited by external auditors.	
5. Charity Tax Back Forms This information is required so that the school may avail of the scheme of tax relief for donations of money received	
<u>To claim the relief</u> , the donor must complete a certificate and forward it to the school to allow it to claim the grossed-up amount of tax associated with the donation. This information is retained by the school in the case of audit by the Revenue Commissioners.	• CHY3/CHY4 tax back forms • Donor name, Address & Telephone Number • PPS Number • Tax Rate • Signature • Gross amount of donation
6. Parent Nominees on Boards of Management This information is required to enable the Board of Management to fulfil its statutory obligations	
Processing undertaken in accordance with the Education Act 1998 and other applicable legislation, including decisions taken for accountability and good corporate governance.	• Name, address and contact details of Parent Nominee • Records in relation to appointment to the Board • Minutes of Board of Management meetings and correspondence to the Board.

Appendix “C”

- Implementing Destruction, Training, bring Your Own Device Security, Password, Cloud Storage Services, Clear Desk, Communication, Personal Data Backup, Business Continuity Management, Business Continuity Plan, Data Breach Management, CCTV, Risk Management, Email, Policies.
- Record of Processing Activities: As a data controller the school is required to prepare a record of any processing activities that it undertakes. The records include the following information (GDPR Article 30):
 - the purposes of the processing.
 - a description of the categories of data subjects and personal data.
 - the categories of recipients to whom the personal data will be disclosed.
 - any transfers to a third country or international organisation, including suitable safeguards.
 - the envisaged time limits for erasure of the different categories of data.
 - a general description of the technical and organisational security measures.
- Risk Assessment: The school as data controller has considered risks that may arise as a consequence of its processing activities. This risk assessment considers the personal data impact assessment, root cause of risk, reassessment.
- Data Protection Impact Assessment (DPIA): A DPIA is a type of risk assessment that is mandatory in specific circumstances (GDPR Article 35). In addition, the school has undertaken a DPIA, in relation to where new processing activity have the potential to have a high impact on individual privacy or rights; the installation of the CCTV system. The purpose of undertaking a DPIA is to ensure that any risks associated with the new processing activity are identified and mitigated in an appropriate manner.
- Security of Processing: As a consequence of having assessed the risks associated with its processing activities, the school has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
- Data Protection by Design: The school aims to apply the highest standards in terms of its approach to data protection. The school has utilised a Privacy by Design approach when any activity that requires the processing of personal data is being planned or reviewed. This meant implementing technical measures (e.g. security) and organisational measures (e.g. policies, recording mechanisms, request forms, compliance documentation, processors instructions and contracts and training).
- Data Protection by Default: A Privacy by Default approach means that minimal processing of personal data is the school's default position. In

practice this meant that only essential data is collected from data subjects, and that within the school, access to this data is carefully controlled and only provided to employees where this is appropriate and necessary.

- Data Processing Agreements: the school has put written contracts in place with organisations that process data on its behalf (as required under GDPR Article 28).
- Data Breach Records: the school will retain records that document its handling of any personal data breaches. These records will clearly set out the facts relating to any personal data breach, its effects and the remedial action taken.
- Staff Awareness and Training: All who are granted access to personal data that is under the control of the school have a duty to observe the data processing principles. The school has provided appropriate information, training and support so that staff gain a clear understanding of these requirements.

1. Lawful Processing

As part of its decision to collect, use or share personal data, the school as Controller has identified the lawful bases applicable to each processing operation.

- Many of school's data processing activities rely on legal obligations. These tasks are undertaken because the school must comply with Irish (or European) law. For example, there is a legislative basis⁶ underpinning the sharing of specific student data with the Department of Education and Skills and other public bodies.
- Another set of data processing activities are undertaken in the public interest i.e. so that the school can operate safely and effectively. For example, the educational profile of the student (literacy competence, language spoken at home etc.) helps the school to target learning resources effectively for the benefit of the student.
- In some situations, such as the use of CCTV, the school relies on its legitimate interests to justify processing. The specific legitimate interests (e.g. health and safety, crime prevention, protection of school property etc.) have been identified and notified to the data subjects⁷.
- Contract will provide a lawful basis for some processing of data by the school. Such as the processing of employee data relies on this lawful basis.
- There is also the possibility that processing may be justified in some circumstances to protect the Vital Interests of a data subject, or another person. For example, sharing some data subject data with emergency services might rely on this lawful basis.

⁶ For example, the Education Act 1998, the Education (Welfare) Act 2000 & the Education for Persons with Special Education Needs Act 2004.

⁷ Data subjects have a right to object to processing that is undertaken based on legitimate interests. In such cases the Controller must demonstrate that there is an overriding need if the processing is to continue.

- Finally, there is the option of using a data subject's consent as the lawful basis for processing personal data. The school will not rely on consent as the basis for processing personal data if another lawful condition is more appropriate. Consent will usually be the lawful basis used by the school to legitimise the publication of student photographs in print publications and electronic media.

2. Consent

Where consent is relied upon as the appropriate condition for lawful processing, then that consent must be freely given, specific, informed and unambiguous. All of these conditions must be satisfied for consent to be considered valid. There are a significant number of restrictions around using consent.

- A separate consent will be sought for each processing activity (together with appropriate guidance as necessary to ensure the data subject is informed).
- When asking for consent, the school ensures that the request is not bundled together with other unrelated matters.
- Consent requires some form of clear affirmative action (Silence or a pre-ticked box is not sufficient to constitute consent). Consent can be provided by means of an oral statement. Consent must be as easy to withdraw as to give.
- A record is kept on how and when consent was given.
- The school has taken steps to ensure the consent is always freely given i.e. that it represents a genuine choice, and that the data subject does not feel under an obligation to consent to processing.
- If the consent needs to be explicit, this means the school will minimise any future doubt about its validity. The school's stores the signed consent statement.

3. Special Category Data

Some personal data is defined as Special Category Data and the processing of such data is more strictly controlled. In a school context this will occur whenever data that relates to Special Needs or Medical Needs is being processed. GDPR Article 9 identifies a limited number of conditions, one of which must be applicable if the processing of special category data is to be lawful. Some of these processing conditions, that are most relevant in the school context, are noted here. (i) Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law. This condition could provide an appropriate basis for processing of data relating to employee and student health e.g. proportionate sharing of special category data to ensure the school is compliant with provisions in health, safety and welfare legislation. (ii) Processing is necessary for the assessment of the working capacity of an employee or for the provision of health or social care or treatment on the basis of Union or Member State law. (iii) Processing is based on Explicit Consent. Where a school is processing biometric data for identification purposes (e.g.

facial image recognition or the use of fingerprint systems) it is unlikely that this processing will be justifiable on any lawful basis other than consent. (And, as a data subject should be able to withhold consent without suffering any detriment, the school will need to provide access to an alternative processing option which is not reliant on biometric data.)

4. Transparency

The school as Controller is obliged to act with *Transparency* when processing personal data. This requires the communication of specific information to individuals in advance of any processing of their personal data.⁸

- (i) Transparency is usually achieved by providing the data subject with a written document known as a *Privacy Notice* or a *Privacy Statement*.⁹ This notice will normally communicate:
 - the name of the controller and their contact details.
 - the categories of personal data being processed.
 - the processing purposes and the underlying legal bases.
 - any recipients (i.e. others with whom the data is shared/disclosed).
 - any transfers to countries outside the EEA (and safeguards used).
 - the storage period (or the criteria used to determine this).
 - the rights of the data subject.¹⁰
- (ii) Transparency information should be provided in a manner that is concise and easy to understand. To best achieve this, the school may use a “layering” strategy to communicate information.¹¹ And, while a written *Privacy Notice* is the default mode, transparency information may also be communicated using other means, for example through the spoken word or through use of pictorial icons or video.
- (iii) Privacy statements (include those used on school websites) should be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data.

⁸ GDPR Articles 13 (or 14)

⁹ Other terms in common use include *Fair Processing Notice* and *Data Protection Notice*. Schools may prepare a number of different Privacy Notices for use in different contexts. For example, a *Website Privacy Notice*, may relate specifically to personal data that is collected via the school website.

¹⁰ In the interests of transparency, the school should ensure that its preferred route for a rights request is identified clearly in *Privacy Notices* and elsewhere e.g. “A data subject wishing to make an access request should apply in writing to the Principal.” Notwithstanding this, school staff should be made aware that valid requests may be submitted in a variety of formats (i.e. not necessarily in writing).

¹¹ For example, where the first point of contact is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13 by way of further, different means, such as by sending a copy of the privacy policy by email and/or sending the data subject a link to the controller’s layered online privacy statement/notice.

5. Purpose Limitation

- (i) Personal data stored by the school has been provided by data subjects for a specified purpose or purposes.¹² Data must not be processed for any purpose that is incompatible with the original purpose or purposes.¹³
- (ii) Retaining certain data (originally collected or created for a different purpose) with a view to adding to a school archive for public interest, scientific or historical research purposes or statistical purposes is acceptable subject to certain safeguards, most particularly the need to respect the privacy of the data subjects concerned.

6. Data Minimisation

As Controller, the school must ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In practice, this principle has a number of important implications illustrated in the examples below.

- (i) The school should ensure, when data is being collected from data subjects, that this is limited to what is necessary for the completion of the duties. For example, where information is being collected from students and parents/guardians, as part of the admissions process, this should be limited to whatever information is needed to operate the admissions process. This means that it is usually not appropriate for the school to seek information about Special Education Needs (SEN) in order to decide whether a place should be offered.¹⁴
- (ii) Data minimisation also requires that the sharing of student data within the school should be carefully controlled. Members of staff may require varying levels of access to student data and reports. Access should be restricted to those who have a defined processing purpose. Staff will not access personal data unless processing is essential to deliver on their role within the school.
- (iii) School staff will necessarily create personal data in the course of their duties. However, employees should ensure that this processing is necessary and appropriate. For example, while it will often be necessary for school staff to communicate information to each other by email, consideration should be given on a case-by-case basis, as to whether it is necessary for personal data to be included in these communications.
- (iv) Data sharing with external recipients should be continuously reviewed to ensure it is limited to that which is absolute necessary. This may mean, for example, that

¹² This purpose is usually communicated to data subjects at the time of collection through providing them with a *Privacy Notice*.

¹³ Data Protection Commission: *Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data. You should ask yourself whether the data subject would be surprised to learn that a particular use of or disclosure of their data is taking place.*

¹⁴ SEN data may be sought where the processing of such data is necessary as part of the Admissions Policy. For example, SEN data may be required to consider whether the student fulfils the criteria for admission to a special education needs unit within a mainstream school.

when the school is seeking professional advice, no personal data will be included in communications unless the disclosure of this information is essential.

7. Storage Limitation

Personal data is kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which it is being processed. Some personal data may be stored for longer periods insofar as the data is being processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

- (i) When deciding on appropriate retention periods, the school's practices will be informed by advice published by the relevant bodies (notably the Department of Education and Skills, the Data Protection Commission, and the school management advisory bodies¹⁵).
- (ii) When documentation or computer files containing personal data are no longer required, the information is disposed of in a manner that respects the confidentiality of the data.
- (iii) Data subjects are free to exercise a "right to erasure" at any time (also known as the "right to be forgotten", see *Data Subject Rights*).
- (iv) Data should be stored in a secure manner that recognises controller obligations under GDPR and the Data Protection Act. This requires the school for example, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

8. Integrity and Confidentiality

Whenever personal data is processed by the school, technical and organisational measures are implemented to safeguard the privacy of data subjects. The school as controller is obliged to take its security responsibilities seriously, employing the most appropriate physical and technical measures, including staff training and awareness. These security procedures should be subject to regular review.

- (i) School employees are required to act at all times in a manner that helps to maintain the confidentiality of any data to which they have access. Guidance and training are important to help identify and reinforce appropriate protocols around data security.
- (ii) The school is legally required to consider the risks to the data subject when any processing of personal data is taking place under its control. Any Risk Assessment should take particular account of the impact of incidents such as accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, the personal data.
- (iii) As well considering the potential severity of any data incident, a risk assessment should also consider the likelihood of any incident occurring. In

¹⁵ see <http://www.dataprotectionschools.ie/en/Data-Protection-Guidelines/Records-Retention/>

this way risks are evaluated on the basis of an objective assessment, by which it is established whether the data processing operations involve a risk or a high risk.¹⁶

- (iv) The follow-on from any risk assessment is for the school to implement appropriate technical and organisational measures that ensure a level of security appropriate to the risk. *These measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected (GDPR Recital 83).*
- (v) As well as processing activities undertaken by staff, the school must also consider the risks associated with any processing that is being undertaken on behalf of the school by other individuals or organisations (Data Processors). Only processors who provide sufficient guarantees about the implementation of appropriate technical and organisational measures can be engaged.
- (vi) The important contribution that organisational policies can make to better compliance with the Accountability principle was previously highlighted. Similarly, the implementation of agreed policies and protocols around data security is very helpful.

¹⁶ The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk (GDPR Recital 76).

APPENDIX “D” - MANAGING RIGHTS 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* in order to facilitate efficient processing of the request. There is no charge for this process.¹⁷
- (ii) 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).¹⁸
- (iii) If requests are manifestly unfounded or excessive¹⁹, 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.
- (iv) 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 searched²⁰). Where appropriate the school may contact the data subject if further details are needed.
- (v) In responding to rights requests (e.g. data access requests) the school will ensure that all relevant manual²¹ and automated systems (computers etc.) are checked.
- (vi) 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.²²
- (vii) The school must be conscious of the restrictions that apply to rights requests.²³ Where unsure as to what information to disclose, the school reserves the right to seek legal advice.²⁴

¹⁷ 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.

¹⁸ 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.

¹⁹ In such circumstances, the school must be able to demonstrate the manifestly unfounded or excessive character of a request.

²⁰ 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.

²¹ Non-automated personal data that is held within a filing system or intended to form part of a filing system (GDPR Article 2).

²² 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.

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

²⁴ 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 inalienable rights of all children. Examples of other factors that

- (viii) 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.
- (ix) 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.

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.
- (iii) Where a request relates to video, then the school may offer to provide the materials in the form of a series of still images. If other people's images cannot be obscured, then it may not prove possible to provide access to the personal data.²⁵

Accountability

- Accountability: Accountability means that compliance with the data protection legislation is recognised as an important Board of Management responsibility as well as one shared by each school employee and member of the wider school community²⁶.
- Demonstrating Compliance: Accountability imposes a requirement on the controller to demonstrate compliance with the other data processing principles. This means that the school retains evidence to demonstrate the actions it has taken to comply with GDPR.
- School Policies: An important way for the school to demonstrate accountability is through the agreement and implementation of appropriate data protection related policies. In addition to publishing a Data Protection Policy it includes the development and implementation of other policies to address the following areas Data Subject's Rights, Personal Data Retention, Data Security, Disposal and

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.

²⁵ Where an image is of such poor quality that it does not relate to an identifiable individual, then it may not be considered to be personal data.

²⁶ The GDPR4schools.ie website identifies some of the GDPR Roles and Responsibilities held by different groups, namely (i) Board of Management (ii) Principal/Deputy Principal (iii) Teaching Staff (iv) Guidance & Medical Support (v) School Administration (vi) SNAs and (vii) Caretaker.

APPENDIX “E”

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://dataprotection4schools.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/generalguidance/gdpr-guidelines-recommendations-best-practices_en
- DES Data Protection Page
<https://www.education.ie/en/The-Department/Data-Protection/Information.html>
- PDST Technology in Education <https://www.pdst.ie/technology-in-education>
- Cyber Security Centre (Ireland) <https://www.ncsc.gov.ie/>
- Cyber Security Centre (UK) <https://www.ncsc.gov.uk/>