St. Munchin's College - Data Protection Policy

Reader Information	Title: Data Protection Policy
Purpose:	To outline the approved St. Munchin's College's management approach to be followed in relation to Data Protection Policy.
Author:	David Quilter
Publication date:	10/04/2019
Target Audience:	All staff, service providers, students, parents, guardians and third parties that have access to the St. Munchin's College information.
Superseded Documents:	All other Data Protection policies.
Review Date:	April 2020
Contact Details:	St. Munchin's College at Corbally Road, Limerick - E-mail: stmunchins@eircom.net

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.

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 shared[1].

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,

[1] JMB's Template Data Protection Policy April 2019.

structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

***'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 processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

'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.

2. Policy statement

2.1 St. Munchin's College located at Corbally Road, Limerickis 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 St. Munchin's 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 St. Munchin's 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 St. Munchin's College's personal data processing functions performed on students, parents / guardians and staff members personal data, and any other personal data that St. Munchin's College may process from other source(s).

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

2.5 St. Munchin's 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 St. Munchin's 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 St. Munchin's College's staff. Any breach of the GDPR will be dealt with by St. Munchin's 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 St. Munchin's 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 St. Munchin's College without having first entered into a data confidentiality agreement, which imposes on the third-party obligations no less onerous than those to which St. Munchin's College is committed, and which gives St. Munchin's College the right to audit compliance with the agreement.

3. Responsibilities and roles under the General Data Protection Regulation

3.1 St. Munchin's 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 St. Munchin's College are responsible for developing and encouraging good information handling practices within St. Munchin's College.

3.3 The Principal being a member of the senior management team, is accountable to St. Munchin's College for the management of personal data within St. Munchin's 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 St. Munchin's College compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that St. Munchin's 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 St. Munchin's College who process or are involved in the processing of personal data.

3.7 St. Munchin's College's Training Policy sets out specific training and awareness requirements in relation to specific roles for the staff of St. Munchin's College generally.

3.8 Staff of St. Munchin's College are responsible for ensuring that any personal data about them and supplied by them to St. Munchin's College is accurate and up-to-date.

3.9 Staff of St. Munchin's 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, and appropriate integrity & confidentiality). St. Munchin's College's policies and procedures are designed to ensure compliance with these principles.

4.1 Personal data must be processed lawfully, fairly and transparently

'Lawful' – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

'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 what information should be available to data subjects, which is covered 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. Information must also be communicated to the data subject in an intelligible form using clear and plain language.

St. Munchin's College's Privacy Notice is set out on its website Https://www.stmunchinscollege.com/
The specific information that must be provided to the data subject must, as a minimum, include:

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 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 Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

4.1.14 Any further information necessary to guarantee fair processing.

4.1.15 Contact details of St. Munchin's 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 St. Munchin's College at Https://www.stmunchinscollege.com/

4.1.18 Automatic Decision Making (Profiling)

4.1.19 Account management, market research or surveys

4.1.20 Email communications policy

4.1.21 Links

4.1.22 Notification of changes

4.2 Personal data can only be collected for specific, explicit and legitimate purposes.

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.

4.3.1 The Controller is responsible for ensuring that St. Munchin's 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, must include a fair processing statement or link to 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 to 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.

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 St. Munchin's College to request data subject to ensure that data held by St. Munchin's College is accurate and up to date. Completion of any registration, application or other form by a data subject should include a statement that the data contained therein is accurate at the date of submission.

4.4.4 Staff/Students/Parents/Guardians or others should be required to notify St. Munchin's College of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of St. Munchin's 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 St. Munchin's 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. If St. Munchin's College decides not to comply with the request, the Controller must respond to the data subject to explain its reasoning

and inform them of their right to complain to the supervisory authority and 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 will not to 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 applicable 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.

4.5.3 The GDPR Controller must 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 must be in writing.

4.5.4 Personal data must 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 St. Munchin's College controlling or processing operations.
In determining appropriateness, the GDPR controller should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or students, parents / guardians) if a security breach occurs, the effect of any security breach on St. Munchin's College itself, and any likely reputational damage including the possible loss of students, parents / guardians trust.

When assessing appropriate technical measures, the GDPR controller should consider the following:

- Password protection access control
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media as well as the secure disposal of personal data stored in storage media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff
- Encryption of personal data stored on devices that leave the organisations premises such as laptops
- Security of local and wide area networks
- Identifying appropriate international security standards relevant to St. Munchin's College.

4.6 When assessing appropriate organisational measures, the GDPR Controller should consider the following: (Governance)

- The appropriate training levels for staff throughout St. Munchin's College;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Consideration of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper-based records;
- Adoption of a clear desk policy;
- Secure Storing of paper-based data;
- Restricting the use of portable electronic devices outside of the workplace;
- Monitoring / Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

Selection of controls to be based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 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. St. Munchin's 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.

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

5. Data subjects' rights

5.1 Data subjects have the following rights regarding data processing, and their personal data that is recorded;

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

5.1.2 To prevent processing likely to cause damage or distress.

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

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

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

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

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

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

5.1.9 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.

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

5.2 St. Munchin's College ensures that data subjects may exercise these rights:

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

5.2.2 Data subjects have the right to complain to St. Munchin's 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.

6. Consent

6.1 St. Munchin's 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.

6.2 St. Munchin's 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.

6.3 St. Munchin's 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.

6.4 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.

6.5 In most instances, the legal processing for processing personal is based on legitimate interest on the part of St. Munchin's College using standard documents.

7. Security of data

7.1 All staff are responsible for ensuring that all personal data that St. Munchin's College holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by St. Munchin's 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.

7.2 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 in line with Disposal and Destruction Policy.

7.3 Care must be taken to ensure that computer screens and terminals are not visible except to authorised Employees/Staff of St. Munchin's 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.

7.4 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.

7.5 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 in accordance with the instructions of the Principal before disposal, where personal or special category data cannot be securely deleted before disposal.

7.6 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.

8. Disclosure of data

8.1 St. Munchin's College must ensure that personal data is not disclosed to unauthorised third parties. All staff should exercise caution when asked to disclose personal data held on data subjects to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of St. Munchin's College's purpose.

8.2 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.

9. Retention and disposal of data

9.1 St. Munchin's 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.

9.2 St. Munchin's 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.

9.3 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 St. Munchin's College has to adhere to in relation to the retention of the personal data.

9.4 St. Munchin's College's personal data retention policy and Disposal and Destruction Policy applies in all cases.

9.5 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.

10. Processor

Where processing of personal data is processed by a processor on behalf of the Controller, a contract 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.

11. Data transfers

11.1 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:

11.1.1 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

11.1.2 Privacy Shield - If St. Munchin's College wishes to transfer personal data from the EU to an organisation in the United States, a check will be required to be carried out to ensure that that the relevant organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify a company as such, the companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the personal data according to a strong set of data protection rules and safeguards. The protection given to the personal data applies regardless of whether the personal data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the EU under that framework.
Assessment of adequacy by the data controller is required when making an assessment of adequacy and the exporting controller should take into account the following factors:

- 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.

11.1.3 Binding corporate rules - St. Munchin's 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 St. Munchin's College would be seeking to rely upon.

11.1.4 Model contract clauses - St. Munchin's College may adopt approved model contract clauses for the transfer of data outside of the EEA if applicable.

11.1.5 Exceptions - In the absence of an adequacy decision, privacy shield membership, 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.

12. Information asset register/data inventory

12.1 St. Munchin's 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. St. Munchin's 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 St. Munchin's College throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

12.2 St. Munchin's College need to be aware of any risks associated with the processing of particular types of personal data.

12.2.1 St. Munchin's College needs to assess the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are to be carried out in relation to the processing of personal data by St. Munchin's College, and in relation to any processing undertaken by other organisations on behalf of St. Munchin's College.

12.2.2 St. Munchin's College shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

12.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, St. Munchin's 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.

12.2.4 Where, as a result of a DPIA it is clear that St. Munchin's 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 St. Munchin's College may proceed must be escalated for review to the GDPR Controller.

12.2.5 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.

12.2.6 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.

13. 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).

14. Compliance Monitoring and Review

St. Munchin's 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.

This Policy was adopted by the Board of Management on Tuesday 22nd October, 2019. It shall be reviewed as part of the school's annual policy review.

Signed _____ Date _____

Chairperson, Board of Management

Signed _____ Date _____

Principal/ Secretary to the Board of Management