Coláiste Mhuire, Mullingar, Co. Westmeath

Data Protection Policy GDPR
April 2021

FOGHLAIM · FÁS · FOIRFIU

Data Protection Policy
January 2020

Coláiste Mhuire
College St, Commons,
Mullingar, Co. Westmeath.

T: (044) 934 4743
E:
reception@cbsmullingar.ie

CIRCULATION SHEET

Client	Coláiste Mhuire
Project Title	Coláiste Mhuire GDPR Project 2020
Document Title	Data Protection Policy

Revisions				
Rev	**Status**	**Approved By**	**Office of Origin**	**Issue Date**
R01	Release	Ark Professional Consultancy Services www.arkservices.ie	Cork	January 2020

Circulation			
Name	**Organisation**	**Issue Date**	**Method**
Principal	Coláiste Mhuire	January 2020	Email

TABLE OF CONTENTS

1 GDPR Compliance Statement

Coláiste Mhuire has at its core a desire to promote and protect the dignity of every member of its community including but not limited to students, staff and parents. This includes respect for the protection of data stored at the school and for the right of access to this data. This policy is informed by these aspirations and also the General Data Protection Regulation of 2016 (GDPR). The policy applies to all school staff, the Board of Management, parents/guardians, students, (including prospective students) their parents/guardians, applicants for positions within the school and service providers with access to school data.

Coláiste Mhuire is aware of its responsibilities as a controller of personal data under GDPR. The school has been briefed as to its scope and implications for our school. All members of staff at Coláiste Mhuire who will be involved in processing personal information will be informed appropriately as to their responsibilities with respect to GDPR in their day to day work.

As a school, we have always been committed to high standards of data protection, information security & privacy. Coláiste Mhuire respects the privacy of students, staff and visitors to the school and is committed to protecting their personal data.

We will safeguard the personal information under our remit and develop a robust data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation of the GDPR.

Our GDPR Principles:

- We will process all personal data fairly and lawfully;
- We will only process personal data for specified and lawful purposes;
- We will endeavour to hold relevant and accurate personal data, and where practical, we will keep this up to date;
- We will not retain personal data for longer than is necessary;
- We will keep all personal data secure;
- We will endeavour to ensure that personal data is not transferred to countries outside of the European Economic Area ('EEA') without adequate protection.

The detailed arrangements for achieving these objectives are set out in the main body of this policy. The Principal together with the Board of Management has overall responsibility for data protection at the school.

This policy requires the co-operation of all staff, visitors, contractors and others to enable Coláiste Mhuire to discharge its responsibilities under the GDPR.

Coláiste Mhuire is committed to upholding the standards outlined in this policy. Sufficient authority and resources, both financial and otherwise, will be made available to enable the school to carry out their responsibilities under the GDPR. All employees will be made aware of and have access to this policy.

The Policy will be reviewed annually in light of experience and future developments within the organisation.

Signed: _____
Chairperson of the Board of Management

Signed: _____
Principal

Date: _____

Date: _____

2 Scope

This policy states the commitment of Coláiste Mhuire to comply with the EU GDPR as a Data Controller and with other relevant legislation. It applies to the personally identifiable information of EU residents such as staff, students, job applicants, and third parties communicating with Coláiste Mhuire as Data Subjects under the purview of the GDPR.

It applies directly to functions of Coláiste Mhuire which collect or process personally identifiable information as part of normal operations. It also applies to external parties who act as Data Processors on behalf of Coláiste Mhuire.

3 Legal Obligations

In the addition to our obligations under GDPR, the implementation of this policy takes into account the school's other legal obligations and responsibilities in the Public Interest. Some of which are directly relevant to data protection:

- Under Section 9(g) of the Education Act, 1998, ensure that parents of a student, or in the case of a student who has reached the age of 18 years, the student, have access in the prescribed manner to records kept by that school relating to the progress of that student in his or her 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 *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).

4 GDPR Principles

4.1 Principle 1: Lawfulness, fairness and transparency

Coláiste Mhuire believes in operating our school fairly and ethically and this will extend to all personal data held for those purposes. Subjects will be informed when data is being collected, and at the same time informed what we will use that data for. We will ensure that appropriate technical and organisational measures are in place to secure that data.

Collection and processing of data will be transparent. Advisory notices and privacy notices relating to data rights will be published as appropriate in plain English and will be structured where relevant to improve accessibility of this information to data subjects. Persons will be clearly advised of their rights also.

4.2 Principle 2: Purpose Limitation

Personal data collected by Coláiste Mhuire will be processed only for the purpose for which it was collected. In the event that this purpose should change, data subjects will be informed within the 30-day regulatory period and consent sought for the change.

4.3 Principle 3: Data Minimisation

Coláiste Mhuire will collect only the minimum quantity of personal data to carry out a particular task. Where appropriate, potential data subjects will be requested not to provide unwanted or inappropriately sensitive personal information.

4.4 Principle 4: Data Accuracy

Coláiste Mhuire will make every effort to ensure that subjects' information is accurate and up to date. Coláiste Mhuire will endeavour to ensure via appropriate levels of staff training that it is transcribed accurately. If it is not possible for subjects to correct their data personally, data can be corrected by contacting Reception.

4.5 Principle 5: Storage Limitation

Coláiste Mhuire will store and retain personal data only while there is a valid and lawful basis to do so. Personal information will be deleted when it is no longer required for the purposes for which it was collected.

Where systems do not allow deletion of all records relating to an individual, records will be anonymised by replacing personal information fields with substituted generic text.

4.6 Principle 6: Integrity & Confidentiality

Personal Data shall be processed securely i.e. in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage. Coláiste Mhuire will use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

4.7 Principle 7: Accountability

Coláiste Mhuire is responsible for and is able to demonstrate compliance with GDPR. This means Coláiste Mhuire will demonstrate that these Data Protection Principles (as outlined here) are met for all Personal Data for which it is responsible.

5 Data Subjects Rights

5.1 Rights of Data Subjects

Coláiste Mhuire recognises the following as the rights of Data Subjects in certain circumstances:

- The right to make Subject Access Requests (SARs);
- The right to have inaccuracies corrected (rectification);
- The right to have information erased (right of erasure);
- The right to restrict the processing of information (restriction);
- The right to be informed on why personal data is processed (notification);
- The right to Data Portability;
- The right to object to processing of personal data (object);
- The right not to be subject to decisions based on automated decision making.

5.2 Right of Access (Also known as a Subject Access Request)

Data Subjects have the Right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information;

Right of access requests must be responded to within one month through the Principal.

5.3 Right to Rectification

Data Subjects are entitled to have their personal data rectified if it is inaccurate or incomplete. If the information in question has been disclosed to a third party the Data Controller must inform them of the request for rectification where possible. The Data Subject is also entitled to be informed of the third parties to whom the data has been disclosed, where appropriate.

Rights to rectification must be responded to within one month.

5.4 Right to Erasure

This Right is also known as the 'Right to be Forgotten'. It enables Data Subjects to request the deletion or removal of personal data where there is no compelling reason for its continued processing by the Data Controller.

The Right to Erasure applies in the following circumstances:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected;
- The processing was based on consent, and the Data Subject has now withdrawn their consent;
- The Data Subject objects to processing and there is no overriding legitimate interest of the Data Controller;
- The data was being unlawfully processed;
- The data must be erased to comply with a legal obligation;

On receipt of this request, we will carry out an assessment of whether the data can be erased without affecting the ability of the School / Department of Education to provide future services to you or to meet it statutory obligations for example under the National Archives Act, 1986.

5.5 Right to Restrict Processing

The Right to Restrict Processing applies in the following circumstances:

- When a Data Subject contests the accuracy of their personal data, then processing should be restricted to storage only until accuracy is verified;
- When a Data Subject objects to processing which is being carried out for the reason of performance of a task in the public interest, then the Data Controller must restrict processing to storage only whilst they consider whether their lawful basis for processing override the Rights and freedoms of the individual;
- When processing is unlawful and a Data Subject opposes the use and requests restriction to storage instead;
- When the Data Controller no longer needs the personal data but the Data Subject requires it for the purpose of, or in the defence of a legal claim.

When this Right is exercised, Coláiste Mhuire will carry out an assessment of whether the data can be restricted without affecting the ability of the School / Department of Education to provide future services to you.

5.6 Right to Data Portability

This Right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one service provider to another in a safe and secure way in a common data format e.g. pdf file.

The Right to Data Portability applies in the following circumstances:

- When the personal data was provided to the controller directly by the Data Subject;
- Where the processing is based on consent or performance of a contract;
- When processing is carried out by automated means.

5.7 Right to Object

Individuals have the Right to object to processing based on:

- Legitimate interest or performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling);
- Processing for the purposes of scientific/historical research and statistics.

5.8 Rights in Relation to Automatic Decision Making and Profiling

This Right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. The Right not to be subject to a decision applies when:

- It is based on automated processing;
- It produces legal/significant effects on the individual not apply if the decision;
- Is necessary for entering into or performance of a contract Is authorised by law;
- Is based on explicit consent;
- Does not have a legal/significant effect on the data subject.

At present there is no automated processing within the Department of Education.

6 Responsibilities

6.1 Board of Management

Implement appropriate technical and organisational measures and be able to demonstrate that data processing is performed in accordance with the Regulation; review and update those measures where necessary considering at all times (with regard to the processing of personal data):

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;

In addition:

- Review and approve the Data Protection Policy;
- Supporting the Principal in the implementation of this policy;
- Review the implementation, effectiveness and compliance with policies, procedures and protocols;
- Ensure Data Protection Issues are an Agenda item at BOM meetings;
- Ensuring that personal data discussed at Board of Management Meetings is kept secure at all times;
- BOM Minutes are handed back to the Principal at the end of each BOM Meeting;

6.2 Senior Management including Principal & Deputy Principal

- Ensure the policy is communicated throughout the school;
- Ensure the policy is implemented throughout the school;
- Ensure personal data relating to students & staff is collected and processed in accordance with this policy;
- Ensure that the basic principles of data protection are explained to staff and parents/guardians. This will be done during staff induction, staff meetings and via the staff handbook.
- Ensure that there are regular updates to data protection awareness, so that data protection is a "living" process aligned to the school's ethos.
- Periodically check data held regarding accuracy.
- Driving privacy and data protection awareness in the school;
- Identifying training needs and arranging for refresher training sessions;
- Escalating appropriate issues to the Board of Management;
- Taking appropriate preventative actions to mitigate the risk of data breaches arising;
- Spearheading the response to any data breach (following the data breach protocol);
- Due diligence of service providers (data processors) prior to any service provider being retained;
- Ensuring adequate assurances of GDPR compliance are obtained.
- Ensuring appropriate written contracts in place with all service providers;
- Ensure that Record-keeping of data protection items is carried out;
- Board of Management (BOM) Meetings:
    - Ensure BOM Minutes and records are kept secure in locked filing cabinets at all times;
    - Ensure that electronic versions of BOM Minutes are kept secure in password protected folders;
    - Ensure minutes that identifies vulnerable persons or particularly sensitive data is anonymized where possible;
    - When emailing minutes, documents will be password protected and sent to a school email address only;
    - Ensure that information is kept secure at all times and that the information is shredded as soon as could be reasonably expected.
- Periodic reviews of all data protection arrangements are carried out.

6.3 Teaching Staff

6.3.1 General

- Read and sign acknowledgement of this policy;
- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty;
- Check that any information that you provide in connection with their employment is accurate and up to date;
- Adherence to high standards of ethics and professionalism in all data entries (e.g. when entering notes about a student on any system);
- Ensure personal data is kept safe and secure, and is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Ensure personal data related to students is accurately processed in accordance with this policy;
- Ensure personal data (particularly sensitive personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion (e.g. if taking personal data to a TUSLA case conference to review a child, ensure the data are stored securely on an encrypted laptop);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with access requests.

6.3.2 Handwritten Notes / Paper Records

- Handwritten Notes can be lost or mislaid (whether in a journal or otherwise).
- Staff are urged to use the functionality provided on VS Ware and other school systems for taking records.
- Staff are advised that they have 4 options when taking handwritten notes:
    - If appropriate, the information on the note should be transferred to VS Ware, and the note shredded or,
    - Note is scanned and saved on the school's server in a secure folder, and the note shredded or,
    - Note is transferred to the students file in a secure filing cabinet in a locked office or
    - If none of the above options are appropriate, then the note is destroyed / shredded as per the retention policy;
- Information required for Parent Teacher Meetings may be printed off VS Ware for that specific purpose providing that the teacher keeps that information secure at all times and that the information is shredded as soon as could be reasonably expected. Under no circumstances will teachers be permitted to take this information off the school premises.

6.3.3 Electronic Records

- When accessing school apps on their own mobile devices and or personal devices, staff will ensure these devices are pin protected, and passwords to school related apps will never be saved / cached in the browser or app. 2 Factor Authentication will be used to access school software systems.
- Should your mobile device get lost / stolen, staff will immediately notify the Principal who will then ensure that login details are reset.
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure that personal data is not visible to others (e.g. never display VS Ware on a projector or leave your computer when logged into VS Ware);
- School servers / cloud have been provided to ensure availability of data, allowing appropriate back-ups to be made, ensuring accountability, transparency, as well as keeping data safe and secure, etc. Staff are urged to use this infrastructure;
- When working with personal data, all staff must ensure that the screens of their computers / tablets / apps are always locked when left unattended;
- Never storing personal data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Only school supplied software is permitted for the recording of personal data at the school.

6.3.4 Emails

- Prepare emails with high levels of diligence and attention to detail i.e. Ensuring that the correct email address is entered; Using "bcc" instead of "to" field where appropriate;
- Limit identifying persons in emails / attachments where at all possible;
- Where emails and attachments contain sensitive personal information, staff are required to encrypt these emails i.e. ensuring only those with a password can open and access the contents of the email.
- Encrypting emails where appropriate for other uses including the use of "Do Not Forward" etc.;
- Attachments containing personal data should be downloaded, stored securely, and then deleted;
- Data should be encrypted before being transferred electronically where appropriate;
- Staff will not save copies of personal data to their own computers, phones, tablets, USB sticks, Hard Drives;

6.3.5 Records

- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;

6.3.6 Social Media

- Never sharing work-related data on unapproved systems (e.g. talking about a student in a teachers WhatsApp group);

6.3.7 Phishing / Malware

- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Never signing the School up to any apps or software relating to school business, or requiring students to engage with apps/software without the prior written approval of the Principal;
- Ensure passwords are unique (e.g. do not use the same password for your Social media account as for your VS Ware account etc);

6.4 Administrators

6.4.1 General

- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty. Read and sign acknowledgement of this policy;
- Prepare post with high levels of diligence and attention to detail. Ensuring that the correct letter is put in the correct envelope. Developing post protocol checklist (e.g. double-checking enclosures, envelope counts, etc);
- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification;
- Keeping Personal Data only as per the Retention Policy to satisfy the permitted uses;
- Ensure data related to students, parents and staff is accurately processed in accordance with this policy;
- Keep the reception area clean and tidy;
- Ensure that personal data is not visible to others (e.g. leaving files on desk);
- Keep personal data out of sight of visitors to reception area;
- Ensure that their computer screen is not visible to visitors at reception;
- Diligence and attention-to-detail when entering data on to the School administrative system;
- Keep the data accurate, complete, and up-to-date;
- Ensuring filing cabinets and office door is kept locked when not in use;
- Keep anti-virus and anti-malware software up to date, install patches when required;
- Respect access-permission levels, never looking into files/records to which you have no genuine employment reason for accessing, adhering to the principle of "need to know";
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;

6.4.2 Subject Access Request

- Identify data subject requests when they are received (by letter, email etc). If received by telephone, asking the person to put their request in writing using the "Subject Access Request Form". Ensuring that all such requests (whether by phone, in person or by email or in writing) are immediately escalated to the Principal without delay;
- Being cautious about requests for information: where a request for personal data is received, asking the requester to verify their identity, ascertaining whether the requester is legally entitled to obtain the personal data;

6.4.3 Email

- Prepare emails with high levels of diligence and attention to detail i.e. Ensuring that the correct email address is entered; Using "bcc" instead of "to" field where appropriate; Encrypting emails where appropriate;
- If emailing to a group, verifying who the members of the group are;
- Be cautious and suspicious if an email asks you to click on links or open an attached document (even if from a familiar sender from a genuine email address);

6.4.4 Phishing / Malware

- Ensure that data are kept safe and secure. Use strong passwords (12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your Social media account as for your VS Ware account etc);
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering;

6.5 Year Heads

- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty;
- Adherence to high standards of ethics and professionalism in all data entries (e.g. preparing summary assessments for teaching staff);
- Take all reasonable measures to secure sensitive personal information regarding students i.e. securing records, ensuring your laptop or desktop computer is password protected and you log out each time you leave it;
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;
- Ensure only relevant teachers are provided with access to sensitive personal information relating to a student;
- Diligence and attention-to-detail when entering data on the student's file (Data accurate, complete, and up-to-date);
- Staff are advised that they have 4 options when taking handwritten notes:
    - If appropriate, the information on the note should be transferred to VS Ware, and the note shredded or,
    - Note is scanned and saved on the school's server in a secure folder, and the note shredded or,
    - Note is transferred to the students file in a secure filing cabinet in a locked office or
    - If none of the above options are appropriate, then the note is destroyed / shredded as per the retention policy;
- School servers / cloud have been provided to ensure availability of data, allowing appropriate back-ups to be made, ensuring accountability, transparency, as well as keeping data safe and secure, etc. Staff are urged to use this infrastructure;
- Ensuring that at all times, Year Head Office & Filing Cabinets are locked when not in use.
- Ensure personal data (particularly sensitive personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop;
- Ensure that disciplinary notes, behavioural reports etc. are never left on desks or in the staff room.
- Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your Social media account as for your school account etc);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with subject access requests.

6.6 SEN Team

- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty;
- Adherence to high standards of ethics and professionalism in all data entries (e.g. preparing summary assessments for teaching staff);
- Take all reasonable measures to secure sensitive personal information regarding students i.e. securing psychological assessments in secure filing cabinets, notes and records, ensuring your laptop or desktop computer is password protected and you log out each time you leave it;
- Where one page Individual Education Leaning Plans (IELP's) are prepared, ensure that access to that folder(s) on the server is password protected to prevent unauthorised access. Ensure that the distribution of IELP's is done so securely;
- Limit identifying persons in emails / attachments where at all possible;
- Where emails and attachments contain sensitive personal information, staff are required to encrypt the attachment to these emails i.e. ensuring only those with a password can open and access the contents of the email.
- Attachments containing personal data should be downloaded, stored securely, and then deleted;
- Staff will not save copies of personal data to their own computers, phones, tablets, USB sticks, Hard Drives;
- Ensuring that at all times the SEN Office & Filing Cabinets are locked when not in use.
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;
- Ensure only relevant teachers are provided with access to sensitive personal information relating to a student;
- Diligence and attention-to-detail when entering data on the student's file (Data accurate, complete, and up-to-date);
- Ensure that any handwritten notes in any notebook are transferred to the students file as soon as possible (to ensure availability of data, ensuring accountability, transparency, as well as keeping data safe and secure, etc);
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Ensure personal data (particularly sensitive personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop;
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your Social media account as for your school account etc);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with subject access requests.

6.7 Care Team

- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty;
- Adherence to high standards of ethics and professionalism in all data entries;
- Take all reasonable measures to secure sensitive personal information regarding students i.e. securing notebooks, plans and files in secure filing cabinets, ensuring the desktop computer is password protected and you log out each time you leave it;
- Where minutes of meetings are prepared, ensure that access to that folder(s) on the server / cloud is password protected to prevent unauthorised access.
- Use Department ID No. to identify students in reports / files / relevant filing systems;
- Limit identifying persons in emails / attachments where at all possible;
- Where emails and attachments contain sensitive personal information, staff are required to encrypt the attachment to these emails i.e. ensuring only those with a password can open and access the contents of the email.
- Attachments containing personal data should be downloaded, stored securely, and then deleted;
- Staff will not save copies of personal data to their own computers, phones, tablets, USB sticks, Hard Drives;
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;
- Ensure only relevant teachers are provided with access to sensitive personal information relating to a student;
- Diligence and attention-to-detail when entering data on the student's file (Data accurate, complete, and up-to-date);
- Ensure that any handwritten notes in any notebook are transferred to the students file as soon as possible (to ensure availability of data, ensuring accountability, transparency, as well as keeping data safe and secure, etc);
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Ensure personal data (particularly sensitive personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop;
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your Social media account as for your school account etc);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with subject access requests.

6.8 Guidance Counsellor

- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty;
- Adherence to high standards of ethics and professionalism in all data entries i.e. notes and record keeping;
- Take all reasonable measures to secure personal information regarding students i.e. securing notes and records, ensuring your laptop or desktop computer is password protected and you log out each time you leave it;
- Ensuring that the office and filing cabinets are locked when not in use.
- Where student files are online, ensure that access to that folder(s) on the server is password protected to prevent unauthorised access.
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;
- Where appropriate, ensure only relevant teachers are provided with personal information relating to a student;
- Ensure that any handwritten notes in any notebook are transferred to the students file as soon as possible (to ensure availability of data, allowing appropriate back-ups to be made, ensuring accountability, transparency, as well as keeping data safe and secure, etc);
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Ensure personal data is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop;
- Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your social media account as for your school account etc);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with subject access requests.

6.9 Website / Social Media Coordinator

- Exercise due care when posting photographs on the school's website and social media channels;
- Ensuring that photos are never shared on social media channels where consent has not been received from the student's parent / guardian;
- When posting photographs, using the student's first name only on our school website, app, on social media or in brochures, yearbooks, newsletters, local and national newspapers and similar school-related productions.
- Deleting photographs off their personal device once emailed / posted on the school's social media channels;
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) for all social media / website accounts and change them regularly.
- Never share log-in credentials i.e. same password for personal social media as school social media accounts.
- Using 2 factor authentication for logging into social media apps and websites.
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;

6.10 Caretaker

- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty;
- Ensure the security of school buildings i.e. locking gates, locking doors;
- Ensure alarms are switched on each evening and working;
- Ensure that only authorised persons have access to School buildings;
- Storage of confidential wastepaper until it is securely shredded;
- Report any personal data breaches immediately to the Principal;
- Comply with and give assistance during audits, spot-checks, and inspections.

6.11 Data Processors (Third Parties with whom the school share personal data)

- Process personal data only on documented instructions from the controller, including with regards to transfers of data outside the EEA;
- Ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Take all measures pursuant to Article 32 on security of processing;
- Respect the conditions for enlisting another processor;
- Assist the controller by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests to exercise data subjects' rights;
- Assist the controller in complying with the obligations in Articles 32–36 (security, data protection impact assessments and breach notification), considering the nature of the processing;
- At the choice of the controller, delete or return all personal data to the controller after the end of the provision of data processing services; and
- Make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

7 Data Protection Policy

7.1 GDPR Awareness

Coláiste Mhuire will ensure that management and staff are aware of GDPR and are trained appropriately to their duties in respect of processing of personal data as per this data protection policy. The training and awareness programme will consist of:

- Briefing to all staff;
- A general email to all staff with the Data Protection Policy;

7.2 Balance of Rights

In using personal data for the operation of the school, we will ensure that we will only use a subject's data if the subject's rights do not outweigh our lawful basis in using that data.

The balance will be assessed by first checking that we have a lawful basis for using the data, and then evaluating whether disproportionate financial, reputational or social harm could be caused to the individual through our use of their data. We will achieve this on an ongoing basis via the Data Protection Policy and Record of Processing methods already explained in this policy.

7.3 Data Protection Impact Assessment

Coláiste Mhuire will carry out and record an impact assessment appropriate in scope to the sensitivity of the personal data being processed. This will identify risks to the data subject, to compliance and to the organisation with respect to GDPR principles. This exercise will be repeated as required i.e. when a change in practices causes us to re-evaluate the impact on data privacy.

7.4 Lawful Processing Criteria

Coláiste Mhuire processes personal data in the pursuance of several lawful processing criteria. In all cases we examine the balance of rights with respect to the use of personal data. It is our objective to align our activities with the rights of the data subject, such that our use of their data is beneficial to the data subject and that any inconvenience or risk to the data subject is minimal in comparison with the benefits there from. We have established our lawful processing criteria in the Data Processing Map in Section 8.

7.5 Storage and Use of Personal Data

The security of personal data relating to students and staff is a very important consideration under the GDPR and is taken very seriously at Coláiste Mhuire. Appropriate security measures will be taken by the school to protect unauthorised access to this data and to the data it is collecting and storing on behalf of the Department of Education and Skills (DES).

A minimum standard of security will include the following measures:

- Access to the information will be restricted to authorised staff on a "need-to-know" basis;
- Manual files will be stored in a relevant filing system, located away from public areas in locked cabinets;
- Computerised data will be held under password protected files;
- Any information which needs to be disposed of will be done so carefully and thoroughly;
- The premises at Coláiste Mhuire are protected by a private security company and is monitored on a 24 hour / 7 day week basis.

7.5.1 Paper based records

Paper based records shall be kept in a secure place where unauthorised people access it. This also applies to data that is usually stored electronically but has been printed out for a valid reason:

- All personnel will ensure that personal data, paper and printouts are not left where unauthorised people could see them;
- When not required, the paper or files will be kept in a relevant filing system in a locked secured filing cabinet or;
- Scanned, transferred to and saved on a password protected folder on the school server / cloud or;
- Data will be shredded and disposed of securely.

7.5.2 Electronic records

When data is stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data will be protected by strong passwords that are changed regularly and never shared between employees;
- Personal Data will only be stored on school supplied equipment / infrastructure i.e. school supplied desktop computers / laptops and school supplied servers, cloud storage;
- Data will be stored on designated drives and servers and will only be uploaded to approved cloud computing services.
- Servers containing personal data will be sited in a secure location.
- Data will be backed up frequently.
- All servers and computers containing data will be protected by approved security software and a firewall.

7.5.3 Use of Student Personal Data

We use student's personal data for purposes including:

- their application for enrolment;
- to provide them with appropriate education and support;
- to monitor their academic progress;
- to care for their health and well-being;
- to care for our staff and students;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an education body;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.
- for the safety of our staff and students and for the protection of personal and school property (use of CCTV).

7.5.4 Use of Staff Personal Data

We use staff personal data for purposes including:

- their application for employment;
- to provide them with appropriate direction and support in your employment;
- to care for their health and well-being;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.;
- for the safety, health & wellbeing of other staff, students and visitors.

Coláiste Mhuire understands that sensitive information may be identified through Garda Vetting. In the event that an employee's Garda vetting raises concerns, the information will be dealt with on a confidential basis. All information pertaining to such a situation will be stored in the same way as other data. The Board of Management will not pass on a copy of a Garda Vetting Form to any other party.

7.6 Sharing Personal Data

From time to time, we may share personal data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, NDTI, An Garda Síochána, HSE, the Department of Social Protection, our Insurance Company, the Revenue Commissioners etc.

The sharing of student personal data and the nature of what is shared depends on various factors. The Government bodies to which we transfer personal data will use that data for their own purposes (including: to verify other information they already hold etc.) and they may aggregate it with other information they already hold about the data subject and the data subject's family. We also share your personal data with other third parties including our insurance company and other service providers (including External Psychologists, Speech Therapists, IT providers, security providers, legal advisors etc). We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

7.7 Special Categories of Data

7.7.1 Children/Students

Special categories of particularly sensitive personal information requires higher levels of protection. The school through the Department of Education may:

- Collect information on ethnic/cultural background of students with the consent of the parent/guardian for statistical analysis and reporting in aggregated format for the purposes of social inclusion and integration.
- Collect data on the religion of the student with the consent of the parent/guardian again for enrolment and statistical purposes.
- Process data related to health in respect of students with special educational needs or a disability for the purpose of ensuring that support services is made available to each child, as defined in section 2 of the Education Act 1998 including psychological services and a level and quality of education appropriate to meeting the needs and abilities of that person.

The Department of Education will only process special categories data relating to children or students for the purposes of allocating resources where this is provided for by way of enactment or the Constitution.

7.7.2 School Staff and Retired School Staff

Special categories of particularly sensitive personal information requires higher levels of protection. The school through the Department of Education may:

- Process data on trade union membership deductions with the consent of the staff member.
- Through the consent of the individual, process religious information where the individual wishes to be addressed by a religious title e.g. Father.
- Process information on sick leave but not the nature of the illness for the purpose of payments to school staff.
- Process data related to health where the occupational health service provides information in respect of applications for retirement on the grounds of ill health.
- Process data related to health when reviewing sample cases as part of an audit of public monies expended in the occupational health service.
- Process information related to religion where a person was or is part of a religious order and the processing of this data is required under the pension schemes.

7.7.3 Photographs of Students

Our school maintains a database of photographs from school events held over the years. It has become customary to take photos of students engaged in activities and events in the interest of creating a pictorial as well as historical record of life at the school. Photographs of students and in some cases including their name, may be published on our school website, app, on social media or in brochures, yearbooks, newsletters, local and national newspapers and similar school-related productions.

Consent is requested from each parent. Should the parent wish to have his/her child's photograph removed from the school website, brochure, yearbooks, newsletters etc. at any time, we will duly comply on receipt of a written request to the school principal. Please note that any images/videos published by the school in yearbooks, newsletters, papers etc. up to this date, will remain in place based on previous consent given. No further images/videos will be published after the date of revocation.

8 Data Processing Map & Retention Policy

Everyone who works for Coláiste Mhuire has a responsibility for ensuring data is collected, stored, and handled appropriately. Each person who handles personal data must ensure that it is handled and processed in line with this policy and the data protection principles.

Personal Data processed at Coláiste Mhuire is summarised in the Data Map along with our legal justification for processing this data and our Retention Policy for same.

Data maps have been prepared to identify our data processing activities. Staff should refer to the Data Map to ensure that personal is stored correctly as per the policy. This shows what data collected, where it is stored, and how it is used.

8.1 Electronic Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D01 G-Suite for Education	Restricted	Google Server	Email Communications. & Cloud Server used in the normal business of the school.	Public Interest. Legal Obligation.	Personal Data incl. Student Data, Staff Data, Policies & Procedures.	Main Office. IT Support. Teachers. Deputy Principal. Principal.	Google's certification under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks includes G Suite and Google Cloud Platform. See Registration here - https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI	Indefinitely.	N/a	**Technical:** Individual Logins for Staff. Authentication by Google G-Suite using username and password. Administrator has full rights to remove files from the Google Drive if needed, and restrict access if needed. Access to G-Suite over Encryption / Https / TLS. TLS is an industry-wide standard based on Secure Sockets Layer (SSL). Google forces HTTPS (Hypertext Transfer Protocol Secure) when users access most services in G Suite. SSL is available for Gmail, Chat, Calendar, Google Groups for Business, Drive, and Sites. **Organisational:** Relevant staff trained on The Data Protection Policy.
D02 Website	Confidential	Squarespace	Provide information to students, parents and staff.	Public Interest. Legal Obligation.	Personal Data incl. Photos of Academic Achievement Awards, Staff Retirements etc.	Parents of Students. Administrators. Teachers. Deputy Principal. Principal.	See Privacy Shield Listing https://www.privacyshield.gov/participant?id=a2zt0000000GnjcAAC	Indefinitely.	N/a	**Technical:** Individual Logins for Staff. Authentication by using username and password. Access to Server over Encryption / Https / TLS. TLS is an industry-wide standard based on Secure Sockets Layer (SSL) technology that encrypts mail for secure delivery. Back-ups are carried out periodically. **Organisational:** Relevant staff trained on The Data Protection Policy.
D03 Local Server	Restricted	Server Room	Local File Storage.	Public Interest. Legal Obligation.	Personal Data incl. Student Data, Staff Data, Policies & Procedures.	Administrators. IT Support. Teachers. Deputy Principal. Principal.	N/a.	Indefinitely.	N/a	**Technical:** Individual Logins for Staff. IT Support has full rights to the network. HEA Net provide robust external network firewalls. Internal Firewall in place (Windows). Back-ups carried out once per month. **Organisational:** Comms Cabinets locked at all times. Relevant staff trained on The Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D04 CCTV	Restricted	Locked and secured in the Deputy Principal's Office.	For the purpose of crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, for the safety of our staff and students and for the protection of personal and school property.	Public Interest.	Video & Images.	Principal. Deputy Principal. Contractor.	N/a	28 Days.	N/a	**Technical:** Images are retained for 28 Days Maximum. CCTV recordings are normally not reviewed unless there is a report of an incident i.e. to gather evidence for an investigation. Otherwise, the CCTV footage is not actively monitored. DPIA conducted. Principal & Contractor can access the images. **Organisational:** Staff briefed on the Data Protection Policy. Individuals can requests copies of CCTV data which contains their personal information. Disclosure of data is covered by the Subject Access Request Procedure outlined in the school's Data Protection Policy which is fully compliant with GDPR.
D05 Photographs	Restricted	Devices of those taking photos. Walls of School. Website.	Documenting, promoting or celebrating through press coverage, websites, prospectuses etc.	Consent.	Images.	Anyone visiting our school or website.	N/a	Indefinitely.	N/a	**Technical:** Only designated staff will take photographs of students engaged in activities and events in the interest of creating a pictorial as well as historical record of life at the school. Images to be deleted from device once developed / posted to website / social media. In the case of website photographs, student names will not appear on the website as a caption to the picture. **Organisational:** Staff briefed on the Data Protection Policy.
D06 Classroom Based Assessments	Restricted	School Devices.	CBA Videos assess research and communication/ presentation skills of Junior Cycle Students. Learning Logs are used in TY for similar purposes.	Legal Obligation.	Video.	Teachers	N/a	Assessment Period.	Deleted from Hard Drive of School Device.	**Technical:** School devices are only permitted for the recording of classroom based assessments and learning logs. Recordings are only kept for the period required to assess the student's work. Once assessment & SLAR Meeting has taken place and the results documented, then the recording will be deleted from the device. Assessment period is no longer than 1 month. **Organisational:** Staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D07 Twitter	Not Restricted	Twitter Server	Provide information to students, parents and staff.	Public Interest.	Personal Data incl. Photos of Academic Achievement Awards, Staff Retirements etc.	Parents of Students. Main Offices. Teachers. Deputy Principal. Principal.	Twitter is certified under the Privacy Shield framework. See https://gdpr.twitter.com/en/dpa.html for more information.	Until we delete our School Twitter Account.	N/a	**Technical:** Individual Logins for Authorised Staff. Authentication by using username and password. Access to Server over Encryption / Https / TLS. TLS is an industry-wide standard based on Secure Sockets Layer (SSL) technology that encrypts for secure delivery. School supplied devices provided to capture photos and post as needed. **Organisational:** Relevant employees trained on Data Protection Policy.
D08 Facebook	Not Restricted	Facebook Server	Provide information to students, parents and staff.	Public Interest.	Personal Data incl. Photos of Academic Achievement Awards, Staff Retirements etc.	Parents of Students. Main Office Staffs. Teachers. Deputy Principal. Principal..	Facebook Inc. is certified under the Privacy Shield framework. See https://www.facebook.com/business/gdpr for more information.	Until we delete our School Facebook Account.	N/a	**Technical:** Individual Logins for Account Administrator. Authentication by Facebook using username and password. Administrator has full rights to remove photos and posts from the Facebook Account if needed. **Organisational:** Relevant staff trained on the Data Protection Policy.

8.2 Student Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D08 Registers & Roll Books	Confidential	**Cloud:** VS Ware	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Student Data incl. Name; Surname; Date of Birth; PPS Number; Address; Parent / Guardian Name; Parent / Guardian Phone Number; Parent Guardian Home address, Mobile, Emergency Contact Person & No., Email, Nationality, Birth Certificate, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History. Photos.	Administrators. Teachers. Deputy Principal. Principal.	N/a	Indefinitely. Archive when class leaves + 2 years.	N/a	**Technical:** Individual Logins for Staff. Authentication by VS Ware System using username and password. Admin Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Fees, Behaviour, Discipline, Docs, Notes, SEN, Classes & Groups, Medical, Account, Enrolment History. Teacher Permissions: (Limited access). Roll Call (AM/PM); Teachers Timetable; Incidents (report student incident); Absent without Leave; Assessment (Exams on system); No access to student personal data. VS Ware uses SSL/TLS protocol that provides secure communications for accessing and updating the record. **Organisational:** Office is locked when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Computers on which records are accessible are password protected and are accessible only to designated staff. Staff briefed on the Data Protection Policy.
D09 State Exam Results	Confidential	**Originals:** Dept of Education. **Paper:** Main Office.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Administrators. Teachers. Deputy Principal. Principal.	N/a	Up to 7 years after the student finishes 6th Year. Following this the student can make an application to the Dept.	Confidential Shredding.	**Technical:** Students can access State Exam Results through the Department's Website. **Organisational:** Staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D010 Application Forms	Confidential	**Paper:** Main Office in locked and secure filing cabinets. **Electronic:** P-Pods. VS Ware.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Student Data incl. Name; Surname; Date of Birth; PPS Number; Address; Parent / Guardian Name; Parent / Guardian Phone Number; Parent Guardian Home address, Mobile, Emergency Contact Person & No., Email, Nationality, Birth Certificate, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History. Photos.	Principal. Deputy Principal. Main Office. Year Heads.	N/a	Up to 7 years after the student finishes 6th Year (or sooner at School's discretion). Those students not enrolling 12 months after registration closing date.	**Paper Copies:** Confidential shredding. **VS Ware:** Securely Delete Student Profile. **P-Pods:** Securely Delete Student Profile.	**Technical:** Individual Logins for Administrators. Authentication by P-Pod & VS Ware System using username and password. Admin Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Fees, Behaviour, Discipline, Docs, Notes, SEN, Classes & Groups, Medical, Account, Enrolment History. VS Ware / P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Electronic Records are backed up periodically. **Organisational:** Office Locked when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Computers on which records are stored are password protected and are accessible only to designated staff. Admin trained on the admin of the P-Pod & VS Ware software. Staff briefed on the Data Protection Policy.
D011 Disciplinary Notes	Confidential	**Cloud:** VS Ware	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data. Incl. Student Name; Class; Teacher; Description of Problem. Frequency of Behaviour; Intervention made to date. Student Reaction to Teacher / Year Head.	Principal. Deputy Principal. Year Head. Teacher.	N/a	Indefinitely. Archive when class leaves + 2 years.	**Paper Copies:** Never Destroy.	**Technical:** Only designated Year Heads & Senior Management have access to this information. **Organisational:** Filing cabinets holding these records will be locked at the end of each day. Relevant employees briefed on the Data Protection Policy and the SEN Policy. Office is locked when not in use.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D012 Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results).	Confidential	**Electronic:** VS Ware	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Administrators. Principal. Deputy Principal. Year Head.	N/a	Up to 7 years after the student finishes 6th Year (or sooner at School's discretion).	**Paper Copies:** Confidential shredding.	**Technical:** Authentication by VS Ware System using username and password. Main Office Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Fees, Behaviour, Discipline, Docs, Notes, SEN, Classes & Groups, Medical, Account, Enrolment History. VS Ware use SSL/TLS protocol that provides secure communications for accessing and updating the record. Electronic Records are backed up periodically. **Organisational:** Offices are locked when not in use. Computers logged out when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Staff briefed on the Data Protection Policy.
D013 End of term/year reports	Confidential	**Electronic:** VS Ware	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Administrators. Principal. Deputy Principal. Year Head.	N/a	Up to 7 years after the student finishes 6th Year (or sooner at School's discretion).	**Paper Copies:** Confidential shredding.	**Technical:** Authentication by VS Ware System using username and password. Main Office Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Fees, Behaviour, Discipline, Docs, Notes, SEN, Classes & Groups, Medical, Account, Enrolment History. VS Ware use SSL/TLS protocol that provides secure communications for accessing and updating the record. Electronic Records are backed up periodically. **Organisational:** Offices are locked when not in use. Computers logged out when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D014 Absences	Confidential	**Electronic:** VS Ware	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Principal. Deputy Principal.	N/a	Up to 7 years after the student finishes 6th Year (or sooner at School's discretion).	**Paper Copies:** Confidential Shredding.	**Technical:** Authentication by VS Ware System using username and password. Main Office Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Fees, Behaviour, Discipline, Docs, Notes, SEN, Classes & Groups, Medical, Account, Enrolment History. VS Ware use SSL/TLS protocol that provides secure communications for accessing and updating the record. Electronic Records are backed up periodically. **Organisational:** Offices are locked when not in use. Computers logged out when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Staff briefed on the Data Protection Policy.
D015 Records of school tours/trips, including permission slips, itinerary reports.	Confidential	**Paper:** Teacher Organising the Trip to provide these to the Deputy Principal's Office. Stored in locked and secure filing cabinets.	Fulfil processing of student records in the course of organising a school trip.	Public Interest. Legal Obligation.	Personal Data incl. Consent Forms.	Administrators. Teachers. Deputy Principal. Principal.	N/a	Indefinitely.	Never Destroy.	**Technical:** Minimal Data including consent collected from the parent / guardian in order to book the trip. In some cases, when school trips are taken abroad student's will be asked to provide necessary information to a travel agent directly i.e. Name, Address, DOB, Passport Number where Data Processing Agreement is in place. **Organisational:** Copies of consent forms kept on file with teacher. Computers on which records are stored are password protected and are accessible only to designated staff.
D016 Garda vetting form & outcome – STUDENTS	Confidential	**Paper:** Student's File in Principal's Office.	Fulfil processing of student records in the course of gaining work experience.	Public Interest. Legal Obligation.	Personal Data.	Placement Employer. Administrators. Teachers. Deputy Principal. Principal.	N/a	Record of outcome retained for 12 months.	**Paper Copies:** Confidential shredding.	**Technical:** Only processed for those over 16 years of age with the consent of a parent / guardian. **Organisational:** School to retain the reference number and date of disclosure on file, which can be checked with An Garda Siochana in the future. Computers on which records are stored are password protected and are accessible only to designated staff.

8.3 Sensitive Personal Data Relating to Students

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D017 Psychological assessments	Confidential	**Paper:** Student's File in SEN Classroom in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Name; Surname; Results of Psychological Assessment.	SEN Coordinator. Administrators. Teachers. Year Head Principal.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** Only designated SEN Coordinators & Senior Management have access to this information. SEN Filing cabinet located in locked office. **Organisational:** Filing cabinets holding these records will be locked at the end of each day. Relevant employees briefed on the Data Protection Policy and the SEN Policy. Office is locked when not in use.
D018 Special Education Needs' files, reviews, correspondence and Individual Education Plans	Confidential	**Paper:** Student's File in SEN Classroom in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Name; Surname; Results of Psychological Assessment. Reviews, correspondence and Individual Education Plans.	Learning Support Teachers. Year Head Teachers. Deputy Principal. Principal.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** Only designated SEN Coordinators & Senior Management have access to this information. SEN Filing cabinet located in locked office. **Organisational:** Filing cabinets holding these records will be locked at the end of each day. Relevant employees briefed on the Data Protection Policy and the SEN Policy. Office is locked when not in use.
D017 Individual Education Learning Plans	Restricted	**Paper:** Student's File in SEN Classroom in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Name; Surname; Results of Psychological Assessment. Reviews, correspondence and Individual Education Plans.	Learning Support Teachers. Year Head Deputy Principal. Principal.	VS Ware	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** Individual Education Learning Plans are prepared electronically using restricted folder access. Individual Logins for Staff. Authentication by username and password. Only designated Teachers have access to this information. Electronic Records are backed up periodically. Computers are password protected and are accessible only to designated staff. **Organisational:** Relevant employees trained on GDPR awareness.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D018 Guidance / Counselling Records	Confidential	**Electronic:** Student's File with Guidance Counsellor in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Sensitive Personal Details.	Guidance Counsellor. CAT 4 Providers. In certain circumstances the appropriate people/agencies or authorities may be informed. The students are made aware of these conditions.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D019 Child protection records	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil our legal obligation under Child Protection Procedures for Primary and Post-Primary Schools 2017.	Public Interest. Legal Obligation.	Personal Data.	Deputy Principal. Principal.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** All incidents are reported to the Principal as per the Child Protection Policy of the school. Principal's Office is locked when not in use. **Organisational:** Relevant staff briefed on the Data Protection Policy and the Child Protection Policy.
D020 Section 29 appeal records	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Public Interest. Establishment, exercise or defence of legal claims.	Personal Data incl. Name; Surname; Address, Home Tel. Number. Daytime Tel. Number. Mobile Tel. Number. Date of Birth. Year / Class of Student. SEN Requirement. Nature of Decision. Particulars associated with the expulsion.	Principal.	N/a	Indefinitely.	**Paper Copies:** Confidential Shredding.	**Technical:** All appeal records are reported to the Principal as per the Policy of the school. Principal's Office is locked when not in use. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D021 Accident Reports	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Public Interest. Establishment, exercise or defence of legal claims.	Personal Data incl. Name; Surname; Address, Particulars associated with an incident.	Administrators. Principal. Deputy Principal.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** All incidents are reported to the Principal as per the Child Protection Policy of the school. Principal's Office is locked when not in use. **Organisational:** Relevant staff briefed on the Data Protection Policy and the Health & Safety Policy.
D022 Enrolment /transfer forms where child is not enrolled or refused enrolment	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	Fulfil processing of student records in the normal course of school operations.	Public Interest. Establishment, exercise or defence of legal claims.	Personal Data incl. Student Data incl. Name; Surname; Date of Birth; PPS Number; Address; Parent / Guardian Name; Parent / Guardian Phone Number; Parent Guardian Home address, Mobile, Emergency Contact Person & No., Email, Nationality, Birth Certificate, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History. Photos.	Administrators. Principal. Deputy Principal.	N/a	12 Months.	**Paper Copies:** Confidential Shredding. **VS Ware :** Securely Delete Student Profile.	**Technical:** Individual Logins for Administrators. Authentication by ESI Net P-Pods System using username and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Computers on which records are stored are password protected and are accessible only to designated staff. Filing cabinets locked and secured when not in use. **Organisational:** Relevant staff trained on the admin of the ESI Net software. Staff briefed on the Data Protection Policy.
D023 Records of complaints made by parents/ guardians	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil processing of student records in the normal admin of school operations.	Public Interest. Establishment, exercise or defence of legal claims.	Personal Data.	Administrators. Principal. Deputy Principal.	N/a	Depends entirely on the nature of the complaint.	If it is child-safeguarding, a complaint relating to teacher-handling, or an accident, then retain indefinitely. Never destroy. If it is a complaint of a more mundane nature (e.g. misspelling of child's name, parent not being contacted to be informed of parent-teacher meeting) or other minor matter, then Up to 7 years after the student finishes 6th Year. Confidential Shredding.	**Technical:** Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Principal's Office is locked when not in use. **Organisational:** Staff briefed on the Data Protection Policy.

8.4 Recruitment Process Records (Unsuccessful Candidates)

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D024 Applications & CVs of candidates called for interview **D025 Database of applications** **D026 Selection Criteria** **D027 Applications of candidates not shortlisted** **D028 Unsolicited job applications** **D029 Candidates shortlisted but not successful** **D030 Interview board marking scheme and notes** **D031 Panel recommendation**	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Recruitment activities of the school.	**Unsuccessful Candidate** Defence of Legal Claim. **Successful Candidate** Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	**Unsuccessful Candidate:** 18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken. **Successful Candidate:** Retain for duration of employment plus 7 years.	**Paper Copies:** Confidential Shredding. **VS Ware :** Securely delete the user's profile.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Note: these suggested retention periods apply to unsuccessful candidates only. They do NOT apply to successful candidates, or candidates who are/were also employees already within your school applying for another post/position. For successful candidates, or candidates who are/were also employees already within your school applying for another post/position, see retention periods set out below.

8.5 Staff Personnel Files

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D032 Applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, training etc. **D033 Application &/CV** **D034 Qualifications** **D035 References** **D036 Interview: database of applications (the section which relates to the employee only)** **D037 Selection Criteria** **D038 Interview Board Marking Scheme & Boards Notes** **D039 Panel recommendation by interview board** **D040 Recruitment Medical (Medmark)**	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D041 Job Specification / Description **D042 Contract/ Conditions of employment** **D043 Probation letters/forms** **D044 POR applications & correspondence (whether successful or not)** **D045 Leave of absence applications** **D046 Job Share** **D047 Career Break**	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D048 Paternity Leave	Confidential	**Paper:** Main Office in locked and secure filing cabinets. **Electronic:** ESI Net	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for 2 years following retirement /resignation or the duration of employment plus 7 years (whichever is the greater).	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by ESI Net system using user-name and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D049 Parental Leave	Confidential	**Paper:** Main Office in locked and secure filing cabinets. **Electronic:** ESI Net	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Must be kept for 8 years - Parental Leave Act 1998 Retain for 8 years or the duration of employment plus 7 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by ESI Net System using user-name and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D050 Force Majeure Leave D051	Confidential	**Paper:** Main Office in locked and secure filing cabinets. **Electronic:** ESI Net	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for 8 years or the duration of employment plus 7 years (whichever is the greater). There is a statutory requirement to retain for 8 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by ESI Net System using user-name and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D052 Carer's Leave	Confidential	**Paper:** Main Office in locked and secure filing cabinets. **Electronic:** ESI Net	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Must be kept for 8 years - Carer's Leave Act 2001 Retain for 8 years or the duration of employment plus 7 years (whichever is the greater).	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by ESI Net system using user-name and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D053 Working Time Act (attendance hours, holidays, breaks)	Confidential	**Paper:** Main Office in locked and secure filing cabinets. **Electronic:** ESI Net	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by ESI Net System using user-name and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D054 Allegations / Complaints	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years Please note the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D055 Grievance and Disciplinary records	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years Please note the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

8.6 Occupational Health Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D056 Sickness Absence Records / Certificates **D057 Pre-Employment Medical Assessment** **D058 Occupational Health Referral** **D059 Correspondence regarding retirement on ill-health grounds**	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for 7 years unless sickness absence relates to an accident / injury / incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.	**Paper Copies:** Confidential Shredding unless sickness absence relates to an accident / injury / incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Individual Logins for OCLS. ESI Net System authenticates using username and password. ESI Net uses SSL/TLS protocol that provides secure communications for updating the record. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Office is locked when not in use. Relevant staff trained on the admin of the ESI NET system. Staff briefed on the Data Protection Policy.
D060 Accident / Injury at Work Reports	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Indefinitely.	Do not destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D061 Medical assessments or referrals	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years There is a statutory requirement to retain for 3 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D062 Sick Leave Records (Sick Benefit Forms)	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years There is a statutory requirement to retain for 3 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Individual Logins for OCLS. ESI Net System authenticates using username and password. ESI Net uses SSL/TLS protocol that provides secure communications for updating the record. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Office is locked when not in use. Relevant staff trained on the admin of the ESI NET system. Staff briefed on the Data Protection Policy.

8.7 Superannuation / Pension / Retirement Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D063 Records of previous service (incl. correspondence with previous employers)	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Indefinitely.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D064 Pension Calculation	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Indefinitely.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D065 Pension increases	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Duration of employment + 7 years or for the life of employee/ former employee plus + 7 years - whichever is the longer.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D066 Salary Claim Forms	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Duration of employment + 7 years or for the life of employee/ former employee plus + 7 years - whichever is the longer.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.

8.8 Government Returns

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D067 **Any returns which identify individual staff/pupils.**	Confidential	**Paper:** Deputy Principal's Office in locked and secure filing cabinets.	Fulfil processing of student records in the normal admin of school operations.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Depends upon the nature of the return. If it relates to pay/pension/ benefits of staff, keep indefinitely as per DES guidelines. If it relates to information on students, e.g. October Returns, Annual Census etc., keep in line with "Student Records" guidelines above.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.

8.9 Board of Management Meeting Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D068 Board agenda and minutes	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil good governance and running of the school in the Public Interest.	Public Interest. Defence of Legal Claim.	Student Personal Data. Staff Personal Data.	Board of Management. Principal. Deputy Principal.	N/a	Indefinitely.	Do Not Destroy	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Desktop computer is encrypted. Office is locked when not in use. **Organisational:** BOM Minutes and records are kept secure in locked filing cabinets at all times; Electronic versions of BOM Minutes are kept secure in password protected folders; Minutes that identifies vulnerable persons or particularly sensitive data is anonymized where possible. BOM minutes are only distributed in paper copy and taken back following the completion of a meeting; Where emailed, the minutes will be password protected and sent to a school email address. Minutes are kept secure at all times and that the information is shredded as soon as could be reasonably expected. Relevant board members & employees briefed on the Data Protection Policy.
D069 School Closure / Amalgamation	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil good governance and running of the school in the Public Interest.	Public Interest. Defence of Legal Claim.	Student Personal Data. Staff Personal Data.	Board of Management. Principal. Deputy Principal. Administrators.	N/a	On school closure, records should be transferred as per Records Retention Policy in the event of school closure / amalgamation. A decommissioning exercise should take place with respect to archiving and recording data.	Do Not Destroy	**Technical:** Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

8.10 Other School Based Reports / Minutes

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D070 Principal's report including staff absences	Confidential	**Electronic:** Principal's Office	Fulfil good governance and running of the school in the Public Interest.	Public Interest. Defence of Legal Claim.	Student Personal Data. Staff Personal Data.	Department. Principal. Deputy Principal.	N/a	Indefinitely.	Do Not Destroy.	**Technical:** Computers on which records are stored are password protected and are accessible only to designated staff. Principal's Office is locked when not in use. **Organisational:** Relevant staff briefed on the Data Protection Policy. Administrative log and does not relate to any one employee in particular: the monthly reports are not structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Not a "relevant filing system".

8.11 Financial Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D071 Audited Accounts	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	School Financial Accounts & Reporting	Public Interest. Legal Obligation.	Board of Management Signatories.	Board of Management. Principal. Deputy Principal. Revenue Commissioner.	N/a	Indefinitely.	Do Not Destroy.	**Technical:** Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system. **Organisational:** Access to Financial Records is limited to authorised personnel i.e. Principal / Deputy Principal, Administrators.
D072 Payroll and Taxation	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	Process Payroll & Taxation.	Public Interest. Legal Obligation. Contractual Obligation.	Staff Personal Data incl. Name, PPSN, Address, Tax Credits.	Board of Management. Principal. Deputy Principal. Revenue Commissioner.	N/a	Indefinitely.	Do Not Destroy.	**Technical:** Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system. **Organisational:** Access to Financial Records is limited to authorised personnel i.e. Principal / Deputy Principal, Administrators.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D073 Invoices / Back Up Records / Receipts	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	School Financial Accounts & Reporting	Public Interest. Legal Obligation. Contractual Obligation.	Vendor Information.	Board of Management. Principal. Deputy Principal. Revenue Commissioner.	N/a	7 years.	Confidential Shredding.	**Technical:** Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system. **Organisational:** Access to Financial Records is limited to authorised personnel i.e. Principal / Deputy Principal, Administrators.

8.12 Promotion Process Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D074 Posts of Responsibility	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Promotion Process of the school.	Public Interest. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Indefinitely.	Do Not Destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D075 Calculation of Service	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Pension Administrators.	Public Interest. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Indefinitely.	Do Not Destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D076 Promotions/POR Boards Master Files	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Promotion Process of the school.	Public Interest. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Indefinitely.	Do Not Destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D077 Promotions/POR Boards assessment report files	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Promotion Process of the school.	Public Interest. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	18 months.	Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D078 POR Appeal Documents	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Promotion Process of the school.	Public Interest. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain original on personnel file, and copy of master & appeal file. Retain for duration of employment + 7 years. Copy on master and appeal file.	Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D079 Correspondence from candidates re feedback	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Promotion Process of the school.	Public Interest. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Depends upon nature of feedback. If feedback is from unsuccessful candidate who is not an employee within the school, keep in line with retention periods in Staff Records above. If feedback is from successful candidate or from unsuccessful candidate who is already an employee within the school, keep in line with "Staff personnel while in employment" above.	Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.

9 Data Protection Communications

9.1 The Data Protection Policy

This document will be made known to all employees and staff as the primary source of Data Privacy Policy at Coláiste Mhuire.

9.2 Coláiste Mhuire Privacy Notice

Coláiste Mhuire's main method of informing data subjects and the general public regarding our use of their data is the Privacy Notice. The Privacy Notice will include at a minimum:

- Identification of Coláiste Mhuire as the controller of personal information;
- A description of the personal information we hold and use;
- An explanation of what we use the information for;
- Who we share the information with;
- Where we store the information;
- How long we keep the information;
- A summary of the data subjects' rights as observed by Coláiste Mhuire;
- Summary technical details regarding information processing (including cookie use);

The Data Privacy Notice will be formatted appropriately for the medium in which it is published.

The Data Privacy Notice is considered an advisory notice regarding Coláiste Mhuire policy, and is not intended to constitute a contract with any person.

9.3 Coláiste Mhuire Website Privacy Notice

Coláiste Mhuire's main method of informing data subjects and the general public regarding its use of their data whilst on our website will be the Website Privacy Notice. The Privacy Notice will include at a minimum:

- Identification of Coláiste Mhuire as the controller of personal information;
- A description of the personal information we hold and use;
- An explanation of what we use the information for;
- Who we share the information with;
- Where we store the information;
- How long we keep the information;
- A summary of the data subject's rights as observed by Coláiste Mhuire;
- Summary technical details regarding information processing (including cookie use);

The Data Privacy Notice will be formatted appropriately for the medium in which it is published.

The Data Privacy Notice is considered an advisory notice regarding Coláiste Mhuire policy, and is not intended to constitute a contract with any person.

9.4 Data Privacy and employees

Employees and contractors will be formally notified of Coláiste Mhuire's position with respect to this policy via a staff briefing.

9.5 Communication plan for Privacy Notices

Coláiste Mhuire will ensure that staff and external parties are informed regarding our use of their data. Any subsequent changes to our policy or practices which affect how user's data is processed will be communicated as per this section.

Employees will be informed directly by email informing of the change, and with attachments or links to supplementary information where required.

Coláiste Mhuire's main vehicle for informing the public of our privacy policy is the data privacy notice which is published on our website. This will be revised as necessary to ensure compliance.

Where certain classes of users (e.g. parents of students) need to be informed more proactively regarding our use of their personal data, we will accomplish this by direct email to those users. This will be carried out in advance of the change going live. Where a change of use requires a response, the lack of a response will not be treated as acceptance.

From time to time it will be necessary to revise the Data Protection Policy as well as associated Privacy Notice in response to changes in regulations or evolution of expectations for compliance.

The Privacy Notice itself contains an advisory to users to check regularly for changes.

10 Third Parties

10.1 General

Coláiste Mhuire avails of the services of outside parties who act as Data Processors on our behalf to assist us in essential school processes.

These include but are not limited to software providers & IT contractors.

Coláiste Mhuire will perform due diligence with respect to any and all such third parties and ensure that:

- The basis of the relationship is clearly defined and falls under Coláiste Mhuire Data Protection Policy;
- A Data Processing Agreement is in place that strengthens our compliance with the GDPR;
- Where data held may not come under GDPR, that a non-disclosure agreement protects personal data;

Only providers who are actively involved in processing personal data will come under scrutiny.

10.2 Transfers of personal data to non-EEA jurisdictions

Our use of third parties may include entities outside the EU/EEA who will process personal data of EU residents on our behalf in the direct exercise of our key organisational processes. Coláiste Mhuire warrants that the use of non-EEA services is an organisational necessity.

In the event we intend to transfer Personal Data to Processor(s) established in a Third Country/ies and if required by the applicable legislation, we shall execute Standard Contractual Clauses. For the avoidance of doubt, in the case of a No-Deal Brexit, the UK will be considered as a Third Country in the meaning of the GDPR for the purpose of this section.

Coláiste Mhuire has identified the following Processors and the adequacy arrangements in place to ensure that these transfers are lawful under GDPR:

Processor	Stored in the EU/EEA?	EU/US Privacy Shield Agreement in place	Standard Contractual Clauses
Facebook	Not always	Yes	N/a
GL Assessments	Yes (as of Dec 2019)	N/a	N/a
Google	Not always	Yes	N/a
Twitter	Not always	Yes	N/a
Wix	Not always	Yes	N/a

11 Data Security Breaches

Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, Coláiste Mhuire will give immediate consideration to informing those affected. Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures.

In appropriate cases, Coláiste Mhuire will also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, Department of Education etc. If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, Coláiste Mhuire may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption of a laptop hard drive) were of a high standard.

All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to Coláiste Mhuire as soon as the data processor becomes aware of the incident.

All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner (DPC) as soon as the school becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial / sensitive personal nature. If there is any doubt related to the adequacy of technological risk-mitigation measures then Coláiste Mhuire will report the incident to the DPC.

Coláiste Mhuire will make initial contact with the DPC within 72 Hours of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact may be by email (preferably), telephone or fax and must not involve the communication of personal data. The DPC will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

Should the DPC request the school to provide a detailed written report of the incident, Coláiste Mhuire will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident;
- a chronology of the events leading up to the loss of control of the personal data;
- and the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the DPC may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the school has not already done so. If necessary, the DPC may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

Even where there is no notification of the DPC, Coláiste Mhuire will keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the school did not consider it necessary to inform the DPC. Such records should be provided to the DPC upon request.

11.1 Data Breach Action Plan

11.1.1 Identification and Initial Assessment of the Incident

- Identify and confirm volumes and types of data affected;
- Establish what personal data is involved in the breach;
- Identify the cause of the breach;
- Estimate the number of data subjects affected;
- Establish how the breach can be contained;

11.1.2 Containment and Recovery

- Establish who within the school needs to be made aware of the breach;
- Establish whether there is anything that can be done to recover the losses and limit the damage the breach could cause;
- Consider partial or complete systems lockdown;
- Establish if it is appropriate to notify affected individuals immediately (for example where there is a high level of risk of serious harm to any individual);

11.1.3 Risk Assessment

- Assessment of volumes and types of data involved will be undertaken and a risk assessment carried out to establish and the risk to data subjects;

11.1.4 Notification

- On the basis of the evaluation of risks and consequences, the Principal will decide whether it is necessary to notify relevant stakeholders i.e.
    - the Gardaí;
    - the Data Subjects affected by the breach;
    - the Data Protection Commissioner;
    - the School's Insurers;
- In accordance with the Data Protection Commissioner's Code of Practice all incidents in which Personal Data has been put at risk will be reported to the Office of the DPC within 72 hours of the school first becoming aware of the breach.
- If, following the assessment described above, it is established that the data breach has been fully and immediately notified to the Data Subjects affected and it affects no more than 100 Data Subjects and it does not include sensitive personal data or personal data of a financial nature, it may not be required to be notified to the DPC. This will be assessed on an individual basis according to the school's policy on Data Breach above, and where there is any doubt, legal advice will be sought.

11.1.5 Evaluation and Response

- Following any serious Breach of Data incident, a thorough review will be undertaken by the school and a report will be made to the Board of Management. This will identify the strengths and weakness of the process and will indicate what areas may need to improve.
- Response may also include updating the Data Protection Policy and retraining staff.

12 Subject Access Requests (SARs)

Coláiste Mhuire recognises the right of data subjects to request information regarding data we hold on them.

12.1 Data Subject Rights

Data Subjects are entitled to obtain, based upon a request made in writing to Coláiste Mhuire using the 'Subject Access Request Form' and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The right of the Data subject to:
    - object to Processing of their Personal Data.
    - lodge a complaint with the Data Protection Authority.
    - request rectification or erasure of their Personal Data.
    - request restriction of Processing of their Personal Data.

12.2 Logging Subject Access Requests

All requests received for access to or rectification of Personal Data must be directed to the Principal, who will log each request as it is received using the Appendix 7: Subject Access Request Register. The data subject will be asked to fill out the Subject Access Request Form. .

12.3 Student making a Subject Access Request

- A student aged eighteen years or older (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves;
- If a student aged eighteen years or older has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student;
- While a student aged from thirteen up to and including seventeen can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is our policy that:
    - If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access;
    - If the information is of a sensitive nature, parental/guardian consent will be sought before releasing the data to the student;
    - If the information would be likely to be harmful to the individual concerned, parental/guardian consent will be sought before releasing the data to the student;
- Each student request for Access to Personal Data will be assessed individually.

12.4 Parents making a Subject Access Request

Where a parent/guardian makes an access request on behalf of his/her child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the parent who requested them. This means that the access request documentation will be sent to the address at which the student is registered on the school's records and will be addressed to the parent subject to the provisions above.

12.5 Third Parties making a Subject Access Request

Where a third party makes an access request on behalf of a child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right).

The student (over 18) or parent / guardian will be required to give permission for the person or organisation making the request on their behalf. Proof of identity will be required to be submitted as part of the Subject Access Request. Once confirmed, the personal data will be sent to the representative at the address provided.

12.6 Responding to Subject Access Requests

A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject.

Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require Coláiste Mhuire to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Coláiste Mhuire cannot respond fully to the request within 30 days, the school shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- The name and contact information of Coláiste Mhuire individual who the Data Subject should contact for follow up.

12.6.1 Protecting Third Parties

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

13 Archiving Personal Data

Coláiste Mhuire will archive personal data we hold for the purpose of retaining that data for no longer than it is outlined in our Data Processing Map. Archiving will take place on an annual basis and will involve the following steps:

1. Identification of records (both electronic and paper) which contain personal data or sensitive personal data and their location (see Data Processing Map & Retention Policy in Section 8);
2. Identification of the purpose(s) for which the data was originally obtained i.e. why did we collect the data (see Data Processing Map & Retention Policy in Section 8);
3. The aim will be to consolidate the records relating to the data subject in one of two locations i.e. VS Ware & the archive (student records) or ESI-NET & the archive (staff records);
4. Appraisal of the records to determine if they contain personal data that a) should be retained for a certain period of time and disposed of or b) should be retained indefinitely for a specific lawful purpose (see Data Processing Map & Retention Policy in Section 8).
5. This step will involve:
    a. Consulting the Retention period as outlined in the Data Map & Retention Policy in Section 8.
    b. Identifying the records for disposal / archiving.
    c. Obtain permission from the Principal to dispose / archive of the records.
    d. Document the disposal / archiving of records.
6. Once established, the data subject's files will be placed in an archive box and will be marked as "For Disposal DD/MM/YY" for records that will be retained for a specific time or "Archive Permanently" for records that will be retained indefinitely.
7. Consultation should also take place with the Principal for advice on record retention periods for certain records as needed.
8. Archived boxes will be held securely in the school's dedicated archive with restricted access.

14 Disposal of Personal Data

Coláiste Mhuire will conduct a regular review of the personal data we hold for the purpose of disposing of redundant personal data. Such a review will take place on an annual basis and will involve the following steps:

1. Identification of records (both electronic and paper) which contain personal data or sensitive personal data (see Data Map & Retention Policy in Section 8);
2. Identification of the purpose(s) for which the data was originally obtained i.e. why did we collect the data (see Data Map & Retention Policy in Section 8);
3. Appraisal of the records to determine if they contain personal data which is no longer necessary for the purposes for which it was originally obtained: This step will involve:
    a. Consulting the Retention period as outlined in the Data Map & Retention Policy in Section 8.
    b. Identifying the records for disposal.
    c. Obtain permission from the Principal to dispose of the records.
    d. Document the disposal of records.
4. Suitable third-party service provider should be contacted to provide a secure erasure and destruction service i.e. confidential shredding through a certified data destruction specialist.
5. Consultation should also take place with the Principal for advice on record retention periods and to ensure that records are disposed of in a safe, secure and appropriate manner.

15 Governance framework

15.1 Supervisory Authority

The Irish Data Protection Commission is our lead supervisory authority under GDPR.

15.2 Monitoring Compliance

Coláiste Mhuire will carry out internal GDPR compliance audits against school policy and procedures.

We will also arrange audits of our compliance by independent third parties at longer intervals.

All audit records will remain confidential to Coláiste Mhuire and will be shown only to regulatory authorities on request. Each audit will, as a minimum, assess:

- Compliance with Data Protection Policy in relation to the protection of Personal Data, including:
  - The assignment of responsibilities;
  - Raising awareness;
  - Training of Employees;
- The effectiveness of Data Protection related operational practices, including:
  - Data Subject rights;
  - Personal Data incident management;
  - Personal Data complaints handling;
- The level of understanding of Data Protection Policies and Privacy Notices;
- The currency of Privacy Notices & Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.

The Data Protection Coordinator, in cooperation with key stakeholders will devise a plan with a schedule for correcting any identified gaps within a defined and reasonable time frame.

15.3 Disciplinary Procedure

Breaches of the GDPR or the school's Data Protection Policy may be treated as a matter for discipline and depending on the seriousness of the breach, and will be dealt with by the Principal in accordance with the School's Disciplinary Procedure.

For breaches of the GDPR Regulations, which do not warrant such action, the employee will be advised of the issue and given a reasonable opportunity to put it right.

In the case of contractors or external service providers, serious breaches of the policies and procedures can and will be deemed grounds for termination of contractual agreements.

Appendix 1: Subject Access Request Form

SECTION 1 – Your details (PLEASE USE BLOCK CAPITALS)

Surname:	
First Name(s):	
Previously known as (if applicable):	
Address:	
Date of birth:	
Telephone number:	
Email address:	

SECTION 2 – Your relationship with Coláiste Mhuire

Are you a current/former* member of staff?	**YES / NO**
If yes, please provide the following details: Period which you were an employee in Coláiste Mhuire i.e. Month & Year.:	
Are you a current/former student of Coláiste Mhuire?	**YES / NO**
If yes, please provide the following details: Period which you were a student in Coláiste Mhuire i.e. Final Year.:	
If neither a student / employee, please indicate your relationship with the Coláiste Mhuire including dates:	

SECTION 3 – PERSONAL DATA REQUESTED

In the box below, please provide as much detail as you can about the personal data you wish to access in order to help us locate it quickly.

In accordance with the GDPR, I request access to the following personal data that I believe Coláiste Mhuire holds about me:
Student Records (Current or Former) **Academic Records incl State Exams Discipline Records Attendance Records Other**
Staff Records (Current or Former) **Personnel File Calculation of Service Other**
If other, please be specific and explicit in your request:

SECTION 4 – FEES

No application fees are required for Subject Access Requests

SECTION 5 – IDENTIFICATION

In order for us to protect the security of personal data, it is necessary for you to provide proof of your identity. Two forms of identification must accompany this form. Acceptable forms of identification include: • **Copy of passport or driving licence** • **Copy of bank statement** • **Staff/student ID Card** • **Copy of utility bill** **Copies are acceptable in most cases; however, we reserve the right to ask to see original documents where necessary. Copies of such documents sent with your access request form will be securely destroyed once we have verified your identity.**

Please complete *either* section 6 *or* section 7 as appropriate

SECTION 6 – DECLARATION OF DATA SUBJECT

I confirm that I am the data subject named in Section 1 and I am requesting access to my own personal data. I understand that the information I have supplied will be used to confirm my identity and help locate the information I have requested. I also understand that it may be used for statistical and monitoring purposes.	
Signed:	**Date:**

SECTION 7 – DECLARATION OF DATA SUBJECT FOR AGENT TO ACT ON THEIR BEHALF
If you wish someone else to submit a data access on your behalf (e.g. family member, solicitor) please complete this section.

I confirm that I am the data subject named in Section 1. I give permission for the person or organisation named below to act on my behalf in relation to my data access request. I have enclosed evidence of my identity referred to in Section 5 and confirm that I want my personal data to be sent to my representative at the address below. I understand that the information I have supplied will be used to confirm my identity and help locate the information I have requested. I also understand that it may be used for statistical and monitoring purposes.	
Signed:	**Date:**

Name of agent:	
Relationship to data subject:	
Address:	
Telephone number:	
Email address:	

RETURNING YOUR COMPLETED FORM:

Please send your completed form (with proof of identity) to: **Principal, Coláiste Mhuire, College St, Commons, Mullingar, Co. Westmeath.** **T: (044) 934 4743 | E: reception@cbsmullingar.ie**

FOR SCHOOL USE ONLY:

Reference No:	**DP/**
Date request received:	
Identity verified:	**YES/NO**
If yes, Original ID supplied in person: **If yes, returned to requester:** **Copy ID attached to request:** **If yes, ID verified and documents shredded by:**	**YES/NO** **YES/NO** **YES/NO** **YES/NO**

Privacy Notice for the Data Subject Access Request

The purposes for which the school processes your data are:

- To verify your identity;
- To verify your address;
- To establish if you are an adult or a child;
- To identify the personal data for which you have requested a copy;

Legal basis:

- Article 12 of the General Data Protection Regulation;
- In the event that you do not provide the information requested on this form it may not be possible to provide a copy of the data requested;

Categories of data subject:

- Requester of data Categories of personal data;
- Identity including any reference numbers provided;
- Address and other contact details;
- Details of their contacts with the Department where relevant to their request;

Further Processing:

- Where the Department intends to further process your data for a purpose other than the purposes listed above, the Department will provide you prior to that further processing with information on that other purpose and with any relevant further information on the processing activity and your data protection rights;

Recipients of the data

- The data provided may be shared with the Data Protection Commissioner where requested by that office;

Storage period

- The data processed will be retained for a period of 3 years and subject to review thereafter;

Third Country

- None of your data will be transferred to a country outside of the European Economic Area i.e. the EU and Norway, Iceland and Liechtenstein;

Rights

- You may also exercise your right to correct your data, seek to restrict how it may be processed or object to how it may be processed. Your data will not be used for automated decision-making or profiling, see http://gdprandyou.ie/wp-content/uploads/2018/03/Rights-of-Individuals-under- the-General-Data-Protection-Regulation.pdf;
- While you have a right to have your data or that of your child deleted, the Department may not be able to agree to your request if it is less than 3 years since you submitted your application;
- You have the right to lodge a complaint with the Data Protection Commissioner, please see www.dataprotection.ie;

Contact Details

- Coláiste Mhuire is the data controller for the processing of your data. If you have any query in respect of this you may contact the Principal or by post to Coláiste Mhuire, College St, Commons, Mullingar, Co. Westmeath.

Appendix 2: Website Data Privacy Notice
(effective 25th May 2018)

This Privacy Notice governs the manner in which Coláiste Mhuire collects, uses, maintains and discloses information collected from users (each, a "User") of the website ("Site"). This Privacy Notice applies to the Site and our school.

Personal Identifiable Information (Post Primary Students)
We collect personal identifiable information from prospective students in a variety of ways in connection with the delivery of education at our school. We will collect personal identifiable information from data subjects when they voluntarily submit such information to us:

Post Primary Student's Data (Lawful Basis: Public Interest, Consent, Legal Obligation):

- Name; Surname; Date of Birth; PPS Number; Address; Nationality; Birth Certificate; Medical Conditions; Programme Subjects & Courses Exemptions; Medium of learning Irish/English; Psychometric Testing Results (where applicable); Religion; Psychological Assessment Results (where applicable); Book Rental Scheme; Transportation Scheme;
- Parent / Guardian Name; Phone Number; Home address; Mobile Number; Emergency Contact Person & No., Email, Mothers Maiden Name; Family Members (current / past); Medical Card;
- Name, Address & Tel. No. of GP, Previous Educational History.
- Photos with classmates, tours, matches, awards etc.
- CCTV Images.
- Classroom based assessments and exam results;
- State Examination Results;

How we use collected information

We use your personal data for purposes including:

- your child's application for enrolment;
- to provide your child with appropriate education and support;
- to monitor your child's academic progress;
- to care for your child's health and well-being;
- to care for our staff and students;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an education body;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.

Personal Identifiable Information (Teaching Staff)
We collect personal identifiable information from prospective staff & staff in a variety of ways in connection with the delivery of education at our school. We will collect personal identifiable information from data subjects when they voluntarily submit such information to us:

Staff & Prospective Staff Data (Lawful Basis: Public Interest, Consent, Contractual Obligation, Legal Obligation):

- Name, Address, Date of Birth, Phone Number;
- PPSN;
- Payroll No.;
- Teaching Council Registration No.;
- Vetting No.;
- Payment details;
- Statutory deductions Voluntary deductions e.g. trade union subscription;
- Service history;
- Leave including Sick leave / Secondments;
- Qualifications & Results (2nd & 3rd Level) & Work Experience;
- Particulars of your cases where you may query the application of the terms and conditions e.g. Contract of indefinite duration;

How we use collected information
We use your personal data (staff) for purposes including:

- your application for employment;
- to provide you with appropriate direction and support in your employment;
- to care for your health and well-being;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.

How we protect your information
We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?
We keep your personal information for a length of time as per our Retention Policy i.e. For post primary & adult education students, this generally means we will retain data for up to 7 years after a student has left the school,

For staff we will retain data for the duration of employment and up to 7 years thereafter. If you apply for a position but you are unsuccessful, will retain your data for up to 18 months after close of the competition.

After this time, your data will be destroyed by confidential shredding or deletion from our school's database.

In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in Coláiste Mhuire Data Protection Policy.

Sharing your personal information
We do not sell or trade personal identification information to others. We may share your data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, NDTI, An Garda Síochána, HSE, the Department of Social Protection, our Insurance Company, the Revenue Commissioners etc.

The sharing of student personal data and the nature of what is shared depends on various factors. The Government bodies to which we transfer personal data will use that data for their own purposes (including: to verify other information they already hold etc.) and they may aggregate it with other information they already hold about the data subject and the data subject's family. We also share your personal data with other third parties including our insurance company and other service providers (including External Psychologists, Speech Therapists, IT providers, security providers, legal advisors etc). We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

Your rights
You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you or a new school if the data is processed automatically (Please note, that we retain only a copy of certain data collected from you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent; and
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this Statement please contact us below.

Personal Identifiable Information (Website)
We may collect personal identification information from users in a variety of ways in connection with activities, services, features or resources we make available on our Site. We will collect personal identification information from Users only if they voluntarily submit such information to us. Users can always refuse to supply personally identification information, except that it may prevent them from engaging in certain Site related activities.

Non-personal Identifiable Information (Website)
We may collect non-personal identification information about users whenever they interact with our Site. Non-personal identification information may include the browser name, the type of computer and technical information about Users means of connection to our Site, such as the operating system and the Internet service providers utilized and other similar information.

Third party websites
Users may find advertising or other content on our Site that link to the sites and services of our partners, suppliers, advertisers, sponsors, licensors and other third parties. We do not control the content or links that appear on these sites and are not responsible for the practices employed by websites linked to or from our Site. In addition, these sites or services, including their content and links, may be constantly changing. These sites and services may have their own privacy policies. Browsing and interaction on any other website, including websites which have a link to our Site, is subject to that website's own terms and policies.

Our use of cookies
Cookies are small pieces of code sent from websites to your device and used to store information by your web browser (see aboutcookies.org). Our use of cookies and other technologies may collect information such as your IP address, operating system, the browser you use and the frequency and length of your visits to our website. This information is treated as your personal information by Coláiste Mhuire under the terms of this Statement.

We use cookies and other technologies to:

- keep track of how you interact with our website;
- target advertising;
- keep track of how you access and download our materials; and
- offer functionality on our website, including social media plug-ins and sharing.

Compliance with children's online privacy protection act
Protecting the privacy of the very young is especially important. For that reason, we never collect or maintain information at our Site from those we actually know are under 13, and no part of our website is structured to attract anyone under 13.

Changes to this privacy policy
Coláiste Mhuire has the discretion to update this privacy policy at any time. When we do, we will revise the updated date at the bottom of this page. We encourage Users to frequently check this page for any changes to stay informed about how we are helping to protect the personal information we collect. You acknowledge and agree that it is your responsibility to review this privacy policy periodically and become aware of modifications.

Links
Some pages of our Website include external links to third party websites. We have no control over and are not responsible for these websites or the use of your information by third parties. You should check the privacy notices on any third party websites to ensure that you are satisfied with their privacy practices, prior to sharing any personal information.

How to contact us
For general queries and requests of any kind, please contact:

Principal
Coláiste Mhuire
College St, Commons, Mullingar, Co. Westmeath.
T: (044) 934 4743
E: reception@cbsmullingar.ie

Appendix 3: Email Data Privacy Notice
Coláiste Mhuire
(for inclusion in all email signatures)

Example (in bold below for effect):

Best regards,

Principal
Coláiste Mhuire
College St, Commons, Mullingar, Co. Westmeath.
T: (044) 934 4743
E: reception@cbsmullingar.ie

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

DATA PROTECTION: We're processing data belonging to you i.e. your email address & name in the Public Interest. For more information please review our Privacy Notice here.

Appendix 4: Enrolment Form Privacy Notice
Coláiste Mhuire
(effective 25th May 2018)

Who is collecting the data
Coláiste Mhuire
College St, Commons, Mullingar, Co. Westmeath.
T: (044) 934 4743
E: reception@cbsmullingar.ie

This Privacy Notice governs the manner in which Coláiste Mhuire collects, uses, maintains and discloses information collected using School Forms.

Personal Identifiable Information (School)
We collect personal identification information from students & prospective students in a variety of ways in connection with the delivery of education at our school. We will collect personal identification information from data subjects only if they voluntarily submit such information to us:

Student's Data (Lawful Basis: Public Interest, Consent, Legal Obligation):

- Name; Surname; Date of Birth; PPS Number; Address; Nationality; Birth Certificate; Medical Conditions; Programme Subjects & Courses Exemptions; Medium of learning Irish/English; Psychometric Testing Results (where applicable); Religion; Psychological Assessment Results (where applicable); Book Rental Scheme; Transportation Scheme;
- Parent / Guardian Name; Phone Number; Home address; Mobile Number; Emergency Contact Person & No., Email, Mothers Maiden Name; Family Members (current / past); Medical Card;
- Name, Address & Tel. No. of GP, Previous Educational History.
- Photos with classmates, tours, matches, awards etc.
- CCTV Images.
- Classroom based assessments and exam results;
- State Examination Results;

How we use collected information
We use your personal data for purposes including:

- your application for enrolment;
- to provide you with appropriate education and support;
- to monitor your academic progress;
- to care for your health and well-being;
- to care for our staff and students;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an education body;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.

How we protect your information
We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?
We keep your personal information for a length of time as per our Retention Policy i.e. For students, this generally means we will retain data for up to 7 years after a student has left the school. After this time, your data will be destroyed by confidential shredding or deletion from our school's database.

In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in Coláiste Mhuire Data Protection Policy which is available to you on request.

Sharing your personal information
We do not sell or trade personal identification information to others. We may share your data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, NDTI, An Garda Síochána, HSE, the Department of Social Protection, our Insurance Company, the Revenue Commissioners etc.

The sharing of student personal data and the nature of what is shared depends on various factors. The Government bodies to which we transfer personal data will use that data for their own purposes (including: to verify other information they already hold etc.) and they may aggregate it with other information they already hold about the data subject and the data subject's family. We also share your personal data with other third parties including our insurance company and other service providers (including External Psychologists, Speech Therapists, IT providers, security providers, legal advisors etc). We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

Your rights
You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you or a new school if the data is processed automatically (Please note, that we retain only a copy of certain data collected from you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent; and
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this Statement please contact us.

Appendix 5: Staff Handbook Privacy Notice
Coláiste Mhuire
(effective 25th May 2018)

Who is collecting the data
Board of Management
Coláiste Mhuire
College St, Commons, Mullingar, Co. Westmeath.
T: (044) 934 4743
E: reception@cbsmullingar.ie

This Privacy Notice governs the manner in which Coláiste Mhuire collects, uses, maintains and discloses information collected throughout the recruitment, hiring and employment of staff.

Personal Data
We collect personal identification information from staff and prospective staff in a variety of ways in connection with your employment at our school.

Staff / Recruitment Data (Lawful Basis: Public Interest, Contractual Obligation, Legal Obligation):

- Name, Address, Date of Birth, Phone Number;
- PPSN;
- Payroll No.;
- Teaching Council Registration No.;
- Vetting No.;
- Payment details;
- Statutory deductions Voluntary deductions e.g. trade union subscription;
- Service history;
- Leave including Sick leave / Secondments;
- Qualifications & Results (2nd & 3rd Level) & Work Experience;
- Particulars of your cases where you may query the application of the terms and conditions e.g. Contract of indefinite duration;

How we use collected information
We use your personal data (staff) for purposes including:

- your application for employment;
- to provide you with appropriate direction and support in your employment;
- to care for your health and well-being;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.

How we protect your information
We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?
We keep your personal information for a length of time as per our Retention Policy i.e. For staff we will retain data for the duration of employment and up to 7 years thereafter. After this time, your data will be destroyed by confidential shredding or deletion from our school's database.

In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in the Coláiste Mhuire Data Protection Policy.

Sharing your personal information
We do not sell or trade personal identification information to others. We may share your data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, An Garda Síochána, HSE, the Department of Social Protection, the Revenue Commissioners etc.

The level of sharing and the nature of what is shared depend on various factors. The Government bodies to which we transfer your personal data will use your personal data for their own purposes (including: to verify other information they already hold about you, etc) and they may aggregate it with other information they already hold about you and your family. We also share your personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc), We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

Your rights
You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you or a new school if the data is processed automatically (Please note, that we retain only a copy of certain data collected from you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent; and
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this statement please contact us.

Appendix 6: Teaching Post Advertisement Privacy Notice
Coláiste Mhuire
(effective 25th May 2018)

Who is collecting the data
Coláiste Mhuire
College St, Commons, Mullingar, Co. Westmeath.
T: (044) 934 4743
E: reception@cbsmullingar.ie

This Privacy Notice governs the manner in which Coláiste Mhuire collects, uses, maintains and discloses information collected throughout the recruitment, hiring and employment of staff.

Personal Identifiable Information
We collect personal identification information from staff and prospective staff in a variety of ways in connection with your employment at our school.

Staff / Recruitment Data (Lawful Basis: Public Interest, Contractual Obligation, Legal Obligation):

- Name, Address, Date of Birth, Phone Number;
- PPSN;
- Payroll No.;
- Teaching Council Registration No.;
- Vetting No.;
- Payment details;
- Statutory deductions Voluntary deductions e.g. trade union subscription;
- Service history;
- Leave including Sick leave / Secondments;
- Qualifications & Results (2nd & 3rd Level) & Work Experience;
- Particulars of your cases where you may query the application of the terms and conditions e.g. Contract of indefinite duration;

How we use collected information
We use your personal data (staff) for purposes including:

- your application for employment;
- to provide you with appropriate direction and support in your employment;
- to care for your health and well-being;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.

How we protect your information
We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?
We keep your personal information for a length of time as per our Retention Policy i.e. For staff we will retain data for the duration of employment and up to 7 years thereafter. If you apply for a position but you are unsuccessful, will retain your data for up to 18 months after close of the competition. After this time, your data will be destroyed by confidential shredding or deletion from our school's database.

In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in Coláiste Mhuire Data Protection Policy.

Sharing your personal information
We do not sell or trade personal identification information to others. We may share your data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, An Garda Síochána, HSE, the Department of Social Protection, the Revenue Commissioners etc.

The level of sharing and the nature of what is shared depend on various factors. The Government bodies to which we transfer your personal data will use your personal data for their own purposes (including: to verify other information they already hold about you, etc) and they may aggregate it with other information they already hold about you and your family. We also share your personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc), We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

Your rights
You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you or a new school if the data is processed automatically (Please note, that we retain only a copy of certain data collected from you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent; and
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this statement please contact us.

Appendix 7: Subject Access Request Register

Ref No:	Name of Data Subject (Print)	Date Initial Contact Received:	Received By: (Print)	Date SAR Form Sent:	Date SAR Form Received:	ID Verified:	Date SAR Processed:	Date SAR Fully Responded to:	Date SAR partially Responded to
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									

Appendix 8: Acknowledgement of the Data Protection Policy

I wish to acknowledge receipt of the Data Protection Policy.

Date	Employee Signature	Blocks

Coláiste Mhuire
An Muileann gCearr

Data Protection Policy 2021

The Board of Management formally adopted this policy on the 15th April 2021.

It shall be reviewed in April 2023.

Signed: Moira Mahon (Apr 20, 2021 09:40 GMT+1)

Ms. Moira Mahon

Chairperson of the Board of Management

Date: Apr 20, 2021