Data Protection Policy

Ballygarvan National School
Ballygarvan,
Cork.

T: 021 488 8390
E: school@ballygarvanns.com

CIRCULATION SHEET

Client	Ballygarvan National School
Project Title	GDPR Project 2019
Document Title	Data Protection Policy

Revisions				
Rev	**Status**	**Approved By**	**Office of Origin**	**Issue Date**
R01	Release	Ark Services Web: www.arkservices.ie	Cork	June 2019

Circulation			
Name	**Organisation**	**Issue Date**	**Method**
Principal	Ballygarvan National School	June 2019	Email

TABLE OF CONTENTS

1 GDPR Compliance Statement

Ballygarvan National School has at its core a desire to promote and protect the dignity of every member of its school community including 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), applicants for positions within the school and service providers with access to school data.

Ballygarvan National School is aware of its responsibilities as a Data Controller of personal data under GDPR. The school has been briefed as to its scope and implications for our school. All Ballygarvan National School staff and employees who will be involved in processing personal information will be informed appropriately as to their duties 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 and transparency. Ballygarvan National School 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 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 Ballygarvan National School to discharge its responsibilities under the GDPR.

Ballygarvan National School 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 staff and 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 school.

Signed: M. Coakley Miriam O'Connell
Chairperson of the Board of Management

Signed: Marival Curtis
Principal

Date: 19th June 2019

Date: 19th June 2019

2 Scope

This policy states the commitment of Ballygarvan National School 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 Ballygarvan National School as Data Subjects under the purview of the GDPR.

It applies directly to functions of Ballygarvan National School 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 Ballygarvan National School.

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, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education;

- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School;

- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring;

- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day;

- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training);

- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers ("SENOs")) such information as the Council may from time to time reasonably request;

- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body;

- Under *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

Ballygarvan National School 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. 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 Ballygarvan National School 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 that change.

4.3 Principle 3: Data Minimisation

Ballygarvan National School 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

Ballygarvan National School will make every effort to ensure that subjects' information is accurate and up to date. Ballygarvan National School 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 the Main Office.

4.5 Principle 5: Storage Limitation

Ballygarvan National School 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. Ballygarvan National School 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

Ballygarvan National School is responsible for, and is able to demonstrate compliance with GDPR. This means Ballygarvan National School 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

Ballygarvan National School 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, Ballygarvan National School 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 to this:

- 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 never disclosed to any unauthorised persons;
- Ensure that handwritten notes are never taken at the BOM Meeting;
- BOM Minutes are handed back to the Principal at the end of each BOM Meeting;
- Where BOM minutes are circulated electronically that this data is kept safe and secure.

6.2 Principal

- Ensure the policy is communicated & implemented throughout the school;
- Ensure personal data is collected and processed in accordance with this policy;
- Ensure that the basic principles of data protection is explained to staff. 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 Meetings:
  - Ensure Meeting Minutes and records are kept secure in locked filing cabinets at all times;
  - Ensure that electronic versions of Meeting Minutes are kept secure in password protected folders;
  - Ensure minutes that identifies vulnerable persons or particularly sensitive data is anonymized where possible.
  - Ensure that information is kept secure at all times and that the information is disposed of as soon as could be reasonably expected.
- Periodic reviews of all data protection arrangements are carried out.

6.3 Administration Staff

6.3.1 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;
- 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 Main Office 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 the Main Office;
- Ensure that their computer screen is not visible to visitors to the Main Office;
- 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;
- 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);
- Keep anti-virus and anti-malware software up to date;
- 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;

6.3.2 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;

6.3.3 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);

6.3.4 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 PayPal account as for your Aladdin account etc);
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering;

6.4 Teaching Staff

6.4.1 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 they 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;
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Ensure personal data (particularly sensitive personal data) is never brought off-site permission from the Principal is first received;
- Assisting the Principal with access requests.

6.4.2 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 Aladdin and other school systems for taking daily records etc.
- Staff are advised that they have 4 options when taking handwritten notes:
    - If appropriate, the information on the note should be transferred to Aladdin, and the note shredded or,
    - Note is scanned and saved on the school's cloud into 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
- Staff are urged to use the functionality provided on Aladdin and other school systems for taking daily notes & records
- Information required for Parent Teacher Meetings may be printed off Aladdin 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.

6.4.3 Electronic Records

- Ensure that personal data is not visible to others (e.g. never display Aladdin on a projector or leave your computer when logged into Aladdin);
- School cloud has 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 / logged out 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 /storage of personal data at the school.

6.4.4 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. Attachments including sensitive personal information should be password protected i.e. ensuring only the recipient(s) 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.;
- Data should be encrypted before being transferred electronically where appropriate;
- Staff will not save copies of personal data to their own personal computers, phones, tablets, USB sticks, Hard Drives;

6.4.5 Records

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

6.4.6 Social Media

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

6.4.7 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;
- 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 PayPal account as for your Aladdin account etc);

6.5 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 PPP's);
- 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 Individual Education Leaning Plans (IELP's) or Personal Pupil Plans (PPP's) are prepared, ensure that access to that folder(s) on the cloud is password protected to prevent unauthorised access. Ensure that the distribution of IELP's / PPP's is done so securely and on a 'needs know' basis.
- Where appropriate, refer to students in PPP's, Support Plans, IEP's, ABC Charts etc. by POD number.
- Ensuring that at all times, the Learning Support Room & 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 is secured in a locked filing cabinet when not in use.
- Ensure Communication logs with parents are documented on the Aladdin software (to ensure availability of data, ensuring accountability, transparency, as well as keeping data safe and secure, etc);
- When sharing information with Post Primary Schools i.e. NCCA Passport, this will be done securely i.e. encrypted email with password protected attachments to the recipients school email address; The password should be provided either verbally in person / on phone but never with the email being sent.
- Retaining only those student SEN records which may be needed to demonstrate the duty of care discharged to students during their time at the school;
- 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;
- 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.);
- 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 PayPal 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 SNA's

- 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 PPP's);
- Take all reasonable measures to secure sensitive personal information regarding students i.e. securing sensitive data relating to students 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 Individual Education Leaning Plans (IELP's) or Personal Pupil Plans 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 / PPP's is done so securely .
- Ensuring that at all times, the SEN Room Office & Filing Cabinets is 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);
- 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.);
- 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 PayPal 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 IT Coordinator

- Supporting the Board of Management and Principal in implementing GDPR best practice at the school;
- Establish and supporting good organisational practices regarding 2 Factor Authentication for logging into school apps.
- Establish and support good organisational practices regarding minimum strength passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) for all school accounts and enforce regular updates / changes for staff;
- Establish and support good organisational practices regarding backups for school supplied desktop and laptop computers.
- Establish and support good organisational practices for encrypting laptops and desktops as needed;
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;

6.8 Website / Social Media Coordinator

- Exercise due care when posting photographs on the school's 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, 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.
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;

6.9 Caretaker & Cleaners

- 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.

6.10 Data Processor

- 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

Ballygarvan National School 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

Ballygarvan National School 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

Ballygarvan National School 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 Map & Processing Activities 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 Ballygarvan National School. 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;

7.6 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 Aladdin;
- Data will be shredded and disposed of securely.

7.7 Electronic records

When data is stored electronically in the school, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts, so far as is reasonably practicable:

- Personal Data will only be stored on school supplied equipment / infrastructure i.e. school supplied desktop computers / laptops and school supplied cloud storage;
- Data will be stored on designated drives and servers and will only be uploaded to approved cloud computing services.
- Data will be protected by strong passwords that are changed regularly;
- Data will be backed up frequently;
- All servers and computers containing data will be protected by approved security software and a firewall.

7.8 Use of Student Personal Data

We use student's personal data for purposes including:

- their application for enrolment;
- to provide our students 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).

7.9 Use of Staff Personal Data

We use staff personal data (staff) 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.

Ballygarvan National School 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.

7.10 Sharing Personal Data

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

The level of sharing student personal data and the nature of what is shared depend on various factors. The Government bodies to which we transfer personal data to may use that personal data for their own purposes (including: to verify other information they already hold about a data subject etc.) and they may aggregate it with other information they already hold about the data subject and their family. We also share your personal data with other third parties including our insurance company and other service providers (including External Psychologists, 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 education to the student's parents/guardians, including results of examinations.

7.11 Special Categories of Data

7.11.1 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.

7.11.2 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.

7.11.3 Photographs of Students

The school maintains a database of photographs of school events held over 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 may be published on our school website or in brochures, yearbooks, newsletters, local and national newspapers and similar school-related productions. In the case of website photographs, the student's name will never appear on the website as a caption to the picture.

Consent is requested from each parent when enrolling with the school. 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.

8 Data Processing Map & Retention Policy

Everyone who works for or with Ballygarvan National School 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 Ballygarvan National School 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 Office 365	Restricted	Microsoft Server	Email Comms. & Cloud Server in the normal business of the school.	Public Interest. Legal Obligation.	Personal Data incl. Student Data, Staff Data, Policies & Procedures.	Main Office. Teachers. Deputy Principal. Principal.	See policy from Microsoft https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located. Note all data transfers are governed by this: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46	Indefinitely.	N/a	**Technical:** Individual Logins for Staff. Authentication by Microsoft using username and password. Access to Email over Encryption / Https / TLS. TLS is an industry-wide standard based on Secure Sockets Layer (SSL) technology that encrypts mail for secure delivery. SSL/TLS protocol that provides secure communications on the Internet for such things as web browsing, e-mail, instant messaging, and other data transfers. Backups are conducted regularly. 2 Factor Authentication available for those accessing Office 365 on their personal device. **Organisational:** Relevant employees trained on GDPR awareness.
D02 Website	Public	Wix	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. Office Staff. Teachers. Principal.	N/a.	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.

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
D03 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.
D04 SMS System	Restricted	Komeer (Amazon Servers).	Communication with School Community.	Public Interest.	Contact Details for School Community.	Principal. Deputy Principal. Main Office. Contractor.	N/a	Indefinitely.	N/a	**Technical:** Individual Logins for Staff. Authentication by Komeer using username and password. Access to System over Encryption / Https / TLS. Data Processing Agreement in place. **Organisational:** Staff briefed on the Data Protection Policy.
D05 CCTV	Restricted	Deputy Principal's locked and secured 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.

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
D06 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.

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
D07 Registers & Roll Books	Confidential	**Cloud:** Aladdin **Paper:** Archive.	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, Country of Birth, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History. Photos.	Office Staff. Teachers. Principal.	N/a	Indefinitely. Archive when class leaves + 2 years.	N/a	**Technical:** Individual Logins for Staff. Authentication by Aladdin using username and password. Aladdin uses SSL/TLS protocol that provides secure communications for accessing and updating the record. System automatically logs users out after a short period of time. Computers on which records are accessible are password protected and are accessible only to designated staff. Data Processing Agreement in place. **Organisational:** Paper records are filed and stored in secure locked cabinets / locked rooms to which only designated staff have access. Staff briefed on the Data Protection Policy.
D08 In House Exam Results	Confidential	**Cloud:** Aladdin.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Teachers. Principal. Support teachers, class teachers.	N/a	7 years after the student leaves the school.	N/a	**Technical:** Individual Logins for Staff. Authentication by Aladdin using username and password. Aladdin uses SSL/TLS protocol that provides secure communications for accessing and updating the record. System automatically logs users out after a short period of time. Computers on which records are accessible are password protected and are accessible only to designated staff. **Organisational:** Paper records are filed and stored in secure locked cabinets / locked rooms 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
D011 Enrolment Forms	Confidential	**Paper:** Records Room in locked and secure filing cabinets. **Electronic:** Some data transferred onto ESI Net / Aladdin.	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, Country of Birth, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History. Photos.	Office Staff. Principal.	N/a	7 years after the student leaves the school.	**Paper Copies:** Confidential shredding. **Aladdin:** Securely Delete Student Profile. **ESI Net:** Securely Delete Student Profile.	**Technical:** Individual Logins for Office Staff. Authentication by ESI Net & Aladdin using username and password. Aladdin / ESI Net 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. Data Processing Agreement in Place with Aladdin. **Organisational:** Office locked when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Admin trained on the admin of the ESI Net / Aladdin software. Staff briefed on the Data Protection Policy.
D012 Disciplinary Notes	Confidential	**Cloud:** Aladdin.	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.	Principal. Teacher. Students. Parents / Guardians.	N/a	Indefinitely. Archive when class leaves + 2 years.	**Paper Copies:** Never Destroy.	**Technical:** Individual Logins for Staff (Authentication by Aladdin) through username and password. Aladdin uses SSL/TLS protocol that provides secure communications for accessing and updating the record. System automatically logs users out after a short period of time. Computers on which records are accessible are password protected and are accessible only to designated staff. Data Processing Agreement in Place with Aladdin. **Organisational:** Paper records are filed and stored in secure locked cabinets / locked rooms 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
D011 End of year reports	Confidential	**Electronic:** Aladdin.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Principal. Teacher. Students. Parents / Guardians.	N/a	7 years after the student leaves the school.	**Paper Copies:** Confidential shredding.	**Technical:** Individual Logins for Staff (Authentication by Aladdin) through username and password. Aladdin uses SSL/TLS protocol that provides secure communications for accessing and updating the record. System automatically logs users out after a short period of time. Computers on which records are accessible are password protected and are accessible only to designated staff. Data Processing Agreement in Place with Aladdin. **Organisational:** Paper records are filed and stored in secure locked cabinets / locked offices to which only designated staff have access. Staff briefed on the Data Protection Policy.
D012 Absences	Confidential	**Electronic:** Aladdin. **Paper:** Sign Out Book Scanned onto server	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Principal. Teacher. Students. Parents / Guardians.	N/a	7 years after the student leaves the school.	**Paper Copies:** Confidential Shredding.	**Technical:** Individual Logins for Staff. Authentication by Aladdin using username and password. Aladdin uses SSL/TLS protocol that provides secure communications for accessing and updating the record. System automatically logs users out after a short period of time. Computers on which records are accessible are password protected and are accessible only to designated staff. Data Processing Agreement in Place with Aladdin. **Organisational:** Paper records are filed and stored in secure locked cabinets / locked rooms to which only designated staff have access. Staff briefed on the Data Protection Policy.

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
D013 Psychological assessments	Highly Confidential	**Electronic:** Aladdin **Paper:** Principal's Office.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Name; Surname; Results of Psychological Assessment.	Learning Support Teacher. Principal.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** Only designated Learning Support Teacher & Principal have access to this information. Coding system in place i.e. Red Star – Health Issues / Yellow - Special Needs. **Organisational:** Filing cabinets holding these records will be locked when not in use. Relevant staff briefed on the Data Protection Policy and the SEN Policy. Room is locked when not in use.
D014 Special Education Needs' files, reviews, correspondence	Highly Confidential	**Electronic:** Aladdin **Paper:** Principal's Office. Learning	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. Principal.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** Only designated Learning Support Teacher & Principal have access to this information. **Organisational:** Filing cabinets holding these records will be locked when not in use. Relevant staff briefed on the Data Protection Policy and the SEN Policy. Room is locked when not in use.
D015 Individual Education Learning Plans	Highly Confidential	**Electronic:** Desktop Computer **Paper:** Learning Support Room.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Name; Surname; Recommended Strategies. Reviews, correspondence and Individual Education Plans.	Learning Support Teachers. Teachers. Principal.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** Computers on which IELPs are prepared are password protected and are accessible only to designated staff. Only designated Learning Support Teacher & Principal have access to this information. **Organisational:** Filing cabinets holding these records will be locked when not in use. Relevant staff briefed on the Data Protection Policy and the SEN Policy. Room 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
D017 Child protection records	Highly Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil our legal obligation under Child Protection Procedures for Primary Schools 2017.	Public Interest. Legal Obligation.	Personal Data.	Principal. Board of Management.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** All incidents are reported to the Principal as per the Child Protection Policy of the school. **Organisational:** Relevant staff briefed on the Data Protection Policy and the Child Protection Policy. Principal's Office is locked when not in use. Records are kept in locked filing cabinets when not in use.
D018 Section 29 appeal records	Highly 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. Board of Management.	N/a	7 years after the student leaves the school.	**Paper Copies:** Confidential Shredding.	**Technical:** All appeal records are reported to the Principal as per the Policy of the school. **Organisational:** Relevant staff briefed on the Data Protection Policy. Principal's Office is locked when not in use. Records are kept in locked filing cabinets when not in use.
D019 Accident Reports	Confidential	**Paper:** Main 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.	Principal. Board of Management. Insurance Company.	N/a	Indefinitely.	**Paper Copies:** Never Destroy.	**Technical:** All incidents are reported to the Principal as per the Child Protection Policy of the school. **Organisational:** Relevant staff briefed on the Data Protection Policy and the Health & Safety Policy. Principal's Office is locked when not in use. Records are kept in locked filing cabinets 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
D020 Enrolment /transfer forms where child is not enrolled or refused enrolment	Confidential	**Paper:** Principal's 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, Country of Birth, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History. Photos.	Board of Management. Principal. Office Staff.	N/a	Destroyed immediately.	**Paper Copies:** Confidential Shredding.	**Technical:** Individual Logins for Office Staff. Authentication by ESI Net System using username and password. ESI Net 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. **Organisational:** Relevant staff trained on the admin of the ESI Net software. Records kept in locked and secure filing cabinets. Staff briefed on the Data Protection Policy.
D021 Records of complaints made by parents / guardians	Highly 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.	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 7 years after the student leaves the school. Confidential Shredding.	**Technical:** Paper records are filed and stored in secure locked cabinets to which only designated staff have access. **Organisational:** Principal's Office is locked when not in use. Records are kept in locked filing cabinets when not in use. 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
D022 Applications & CVs of candidates called for interview **D023 Database of applications** **D024 Selection Criteria** **D025 Applications of candidates not shortlisted** **D026 Unsolicited job applications** **D027 Candidates shortlisted but not successful** **D028 Interview board marking scheme and notes** **D029 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.	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. **Aladdin :** Securely delete the user's profile.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Principal's Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. 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
D030 Applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, training etc.	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.	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. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Principal's Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. Relevant staff briefed on the Data Protection Policy.
D031 Application &/CV										
D032 Qualifications										
D033 References										
D034 Interview: database of applications (the section which relates to the employee only)										
D035 Selection Criteria										
D036 Interview Board Marking Scheme & Boards Notes										
D037 Panel recommendation by interview board										
D038 Recruitment Medical (Medmark)										

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
D039 Job Specification / Description **D040 Contract/ Conditions of employment** **D041 Probation letters/forms** **D042 POR applications & correspondence (whether successful or not)** **D043 Leave of absence applications** **D044 Job Share** **D045 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.	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. 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. Principal's Office is locked when not in use. Filing cabinets holding these records will be locked when not in use.
D046 Paternity Leave	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.	Office Staff. 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. 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. **Organisational:** Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. 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
D047 Parental Leave	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets. **Electronic:** Main Office – Data entry. OLCS (Main Office).	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.	Office Staff. 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. SSL/TLS protocol provides secure communications for accessing and updating the record. Computers on which records are stored / accessed are password protected and are accessible only to designated staff. **Organisational:** Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. Relevant staff briefed on the Data Protection Policy.
D048 Force Majeure Leave D049	Confidential	**Paper:** Staff Files in Principal's Office in locked and secure filing cabinets. **Electronic:** OLCS.	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.	Office Staff. 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. SSL/TLS protocol provides secure communications for accessing and updating the record. Computers on which records are stored / accessed are password protected and are accessible only to designated staff. **Organisational:** Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. 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
D050 **Carer's Leave**	Confidential	**Paper:** Staff Files in Principal's Office in locked and secure filing cabinets. **Electronic:** OLCS.	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.	Office Staff. 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. SSL/TLS protocol provides secure communications for accessing and updating the record. Computers on which records are stored / accessed are password protected and are accessible only to designated staff. **Organisational:** Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. Relevant staff briefed on the Data Protection Policy.
D051 **Working Time Act (attendance hours, holidays, breaks)**	Confidential	**Paper:** Staff Files in Principal's Office in locked and secure filing cabinets. **Electronic:** OLCS.	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.	Office Staff. 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. SSL/TLS protocol provides secure communications for accessing and updating the record. Computers on which records are stored / accessed are password protected and are accessible only to designated staff. **Organisational:** Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. 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 Allegations / Complaints	Highly Confidential	**Paper:** Staff Files in 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.	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. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Principal's Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. Relevant staff briefed on the Data Protection Policy.
D053 Grievance and Disciplinary records	Highly Confidential	**Paper:** Staff Files in 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.	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. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Principal's Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. 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
D054 Sickness Absence Records / Certificates **D055 Pre-Employment Medical Assessment** **D056 Occupational Health Referral** **D057 Correspondence regarding retirement on ill-health grounds**	Confidential	**Paper:** Staff Files in 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.	Office Staff. 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 OLCS. 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.
D058 Accident / Injury at Work Reports	Confidential	**Paper:** Staff Files in 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.	N/a	Indefinitely.	Do not destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Principal's Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. 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
D059 Medical assessments or referrals	Confidential	**Paper:** Staff Files in 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.	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. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Principal's Office is locked when not in use. Filing cabinets holding these records will be locked when not in use. Relevant staff briefed on the Data Protection Policy.
D060 Sick Leave Records (Sick Benefit Forms)	Confidential	**Paper:** Staff Files in 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.	Office Staff. 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 OLCS. 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
D061 Records of previous service (incl. correspondence with previous employers)	Confidential	**Electronic:** ESI Net / Pod **Paper:** Archive	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.	Office Staff. 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 OLCS. 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:** Archive is locked when not in use. Relevant staff trained on the admin of the ESI NET system. Staff briefed on the Data Protection Policy.
D062 Pension Calculation	Confidential	**Electronic:** ESI Net / Pod **Paper:** Archive	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.	Office Staff. 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 OLCS. 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:** Archive is locked when not in use. Relevant staff trained on the admin of the ESI NET system. 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
D063 Pension increases	Confidential	**Electronic:** ESI Net / Pod **Paper:** Archive	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.	Office Staff. 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 OLCS. 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:** Archive is locked when not in use. Relevant staff trained on the admin of the ESI NET system. Staff briefed on the Data Protection Policy.
D064 Salary Claim Forms	Confidential	**Electronic:** ESI Net / Pod **Paper:** Archive	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.	Office Staff. 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 OLCS. 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:** Archive is locked when not in use. Relevant staff trained on the admin of the ESI NET system. Staff briefed on the Data Protection Policy.

8.8 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
D065 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. Office Staff.	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 password protected. Principal's 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. Minutes are kept secure at all times and that the information is shredded as soon as could be reasonably expected. Relevant employees briefed on the Data Protection Policy.

8.9 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
D066 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. 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 only.
D067 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.	Office Staff.	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 only.

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 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.	Principal. Office Staff.	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 only.

8.10 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
D069 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.	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.
D070 Calculation of Service	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Pension Admin.	Public Interest. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Office Staff. 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.
D071 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.	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
D072 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.	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.
D073 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.	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.
D074 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.	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 Notices

9.1 When is a Data Protection Notice required?

Where information is being collected directly from an parent / teacher, a Data Protection Notice must be provided at the point at which the data is collected.

- Where information is obtained from another source, a Data Protection Notice must be provided:
- If personal data is to be used to communicate with the data subject, at the latest at the time of the first communication with the data subjects;
- If disclosure to another recipient is envisaged, at the latest when personal data is first disclosed.

9.2 What needs to be included in a Data Protection Notice?

Data Protection Notices must contain specific information which informs data subjects of:

- Who is collecting the data;
- Why it is being collected;
- What legal basis is being relied upon to process the data;
- How it will be processed;
- How long it will be kept for;
- Who it will be disclosed to.

9.3 What rights people have in relation to their own data?

Individuals will also be made aware of their rights as per Section 5.

- 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.

10 Data Protection Communications

10.1 The Data Protection Policy

This document will be made known to all board of management members, parents (via the website), employees and staff as the primary source of Data Privacy Policy at Ballygarvan National School.

10.2 Ballygarvan National School Privacy Statement

Ballygarvan National School's main method of informing data subjects and the general public regarding our use of their data is the Privacy Statement. The privacy statement will include at a minimum:

- Identification of Ballygarvan National School 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 Ballygarvan National School;
- Summary technical details regarding information processing (including cookie use);

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

The Data Privacy Statement is considered an advisory notice regarding Ballygarvan National School policy, and is not intended to constitute a contract with any person.

10.3 Ballygarvan National School Website Privacy Statement

Ballygarvan National School'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 Statement. The privacy statement will include at a minimum:

- Identification of Ballygarvan National School 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 Ballygarvan National School;
- Summary technical details regarding information processing (including cookie use);

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

The Data Privacy Statement is considered an advisory notice regarding Ballygarvan National School policy, and is not intended to constitute a contract with any person.

10.4 Data Privacy and employees

Employees and staff will be formally notified of Ballygarvan National School's position with respect to this policy via a staff briefing.

10.5 Communication plan for Privacy Notices

Ballygarvan National School 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.

Ballygarvan National School'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/guardians 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 data privacy statement itself contains an advisory to users to check regularly for changes.

11 Third parties

11.1 General

Ballygarvan National School 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.

Ballygarvan National School 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 Ballygarvan National School 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.

11.2 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 school processes. Ballygarvan National School warrants that the use of non-EEA services is a school necessity. In these cases, Ballygarvan National School has identified the following:

Processor	Stored in the EU/EEA?	EU/US Privacy Shield
Microsoft	Not always	Yes
Wix	Not always	Yes
Aladdin	Yes	N/a
ESI Net	Yes	N/a
Komeer (Amazon Servers)	Not always	Yes
Twitter	Not always	Yes

12 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, the school must 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, the school 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, the school 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) were of a high standard.

All incidents of loss of control of personal data in manual or electronic form by a data processor (contractor or service provider) must be reported to the school 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 management 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 - the school will report the incident to the DPC.

The school will make initial contact with the DPC within 72 Hours of becoming aware of the incident, outlining the circumstances surrounding the incident using the online reporting system. 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, the school 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 their enforcement powers to compel appropriate action to protect the interests of data subjects.

Even where there is no notification of the DPC, the school 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.

12.1 Data Breach Action Plan

12.1.1 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;

12.1.2 Contain and Recover

- 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;
- 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);

12.1.3 Risk to Data Subjects

- A detailed analysis of volumes and types of data involved will be undertaken to establish the risk to data subjects;

12.1.4 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.

12.1.5 Evaluation and Response

- Following any serious Breach of Data incident, a thorough review will be undertaken by the Principal and a report will be prepared. 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.

13 Subject Access Requests (SARs)

Ballygarvan National School recognises the right of data subjects to request information regarding data we hold on them.

13.1 Data Subject Rights

Data Subjects are entitled to obtain, based upon a request made in writing to Ballygarvan National School 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.

13.2 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.

13.3 Parents making a Subject Access Request

Where a parent/guardian makes an access request on behalf of his/her child (a current or former student), 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 / guardian 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 / guardian subject to the provisions above.

13.4 Third Parties making a Subject Access Request

Where a third party makes an access request on behalf of a child (the parent of guardian) the right of access is a right of the data subject (i.e. it is the student's right).

The 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.

13.5 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 Ballygarvan National School to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Ballygarvan National School cannot respond fully to the request within 30 days, the Principal 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 Ballygarvan National School individual who the Data Subject should contact for follow up.

13.6 Grounds for Exemption / Refusing a Subject Access Request

Where a request is deemed manifestly unfounded/excessive, the school at its discretion may refuse to honour the request. Situations where this may arise include, but is not limited to:

- Multiple requests from the same person (the school can wait a reasonable interval before having to respond to the exact same data access request);
- The person requesting this data can readily access the data being requested;
- Data relating to the investigation of a criminal offence (where it would prejudice the investigation);
- Where legal professional privilege applies to the data (e.g. communications between the organisation and its legal advisors for the purposes of obtaining legal advice);
- A disproportionate effort would be involved;

13.7 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.

14 Archiving Personal Data

Ballygarvan National School 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. Aladdin & 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 archiving.
    c. Obtain permission from the Principal to archive the records.
    d. Document the 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.

15 Disposal of Personal Data

Ballygarvan National School will conduct a regular review of the personal data they hold for the purpose of disposing of redundant personal data. It is recommended that such a review should take place on an annual basis. Such a review should involve the following steps:

9. Identification of records (both electronic and paper) which contain personal data or sensitive personal data (see Data Map & Retention Policy in 8);
10. 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);
11. 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.
12. 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.
13. 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.

16 Governance framework

16.1 Supervisory authority

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

16.2 Monitoring Compliance

Ballygarvan National School 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 Ballygarvan National School 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 Statements & 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.

16.3 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.