Data Protection Policy

Catholic University School
89 Lower Leeson Street, Dublin 2.
T: 01 775 6800
E: office@cus.ie

Issued By
The Ark HQ™

Date Issued
September 2024

Data Protection Policy

Document Title

Data Protection Policy

Revisions

No.	Status	Author(s)	Office	Issue Date
Rev 01	Release	The Ark HQ™	Cork	December 2019
Rev 01	Release	The Ark HQ™	Cork	September 2024

Circulation

Position	Office	Issue Date	Method
Senior Management	Catholic University School	September 2024	Email
Board of Management	Catholic University School	September 2024	Email
Staff	Catholic University School	September 2024	Email

Table of Contents

1. GDPR Compliance Statement 4
2. Scope 5
3. Legal Obligations 6
4. GDPR Principles 7
5. Data Subject's Rights 8
6. Responsibilities – Board of Management 10
7. Responsibilities – Senior Management 10
8. Responsibilities – Teachers 11
9. Responsibilities – Administrators 13
10. Responsibilities – Year Heads 14
11. Responsibilities – AEN Department including SNA's 15
12. Responsibilities – Guidance Counsellor 16
13. Responsibilities – Student Support Team 17
14. Responsibilities – Contractors, Maintenance Teams etc. 18
15. Responsibilities – Data Processors etc. 18
16. GDPR Awareness 18
17. Balance of Rights 19
18. Data Protection Impact Assessments 19
19. Lawful Processing Criteria 19
20. Storage & Processing of Personal Data 20
21. Sharing Personal Data 22
22. Special Categories of Personal Data – Students / Prospective Students 22
23. Special Categories of Personal Data – Staff 23
24. Photographs and video 24
25. Data Processing Map & Retention Schedule 27
26. Electronic Records 28
27. Student Records 31
28. Sensitive Personal Data 35
29. Recruitment Process Records (Unsuccessful Candidates) 38
30. Staff Personnel Files 39
31. Occupational Health Records 43
32. Superannuation / Pension / Retirement Records 45
33. Government Returns 46
34. Board of Management Meeting Records 47
35. Other School Based Reports / Minutes 48
36. Financial Records 49
37. Promotion Process Records 50
38. Data Protection Communications – Data Protection Policy 52
39. Data Protection Communications – Privacy Notices 52
40. Data Protection Communications – Website Privacy Notice 53
41. Communication Plan for Privacy Notices 53
42. Third Parties – Data Processors 54
43. Third Parties – Transfers of Personal Data to non-EEA jurisdictions 54
44. Data Security Breaches 55
45. Data Security Breach – Action Plan 56
46. Subject Access Requests 57
47. Archiving Personal Data 60
48. Disposal of Personal Data 61
49. Governance 62
50. Data Protection Policy Acknowledgement 63

Data Protection Policy

This policy is informed by these aspirations and also the General Data Protection Regulation of 2016 (GDPR).

Catholic University School has at its core a desire to promote and protect the dignity of every member of its community including but not limited to students, staff and Parent(s) / Guardian(s). This includes respect for the protection of personal 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, parent(s) / guardian(s), students, (including prospective students) their parent(s) / guardian(s), applicants for positions within the school and service providers with access to school data.

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

As a school, we have always been committed to high standards of data protection, information security & privacy. Catholic University 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 data under our remit and develop a robust data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation of the GDPR.

Our GDPR Principles:

- We will process all personal data lawfully, fairly and transparently.
- 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 Catholic University School to discharge its responsibilities under the GDPR. Catholic University 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 employees will be made aware of and have access to this policy. The Policy will be reviewed annually in light of experience and future developments within the organisation.

Signed: _____
Chairperson Board of Management

Signed: _____
Principal

Date: _____

Date: _____

2. Scope

This policy states the commitment of Catholic University 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 Catholic University School as Data Subjects under the purview of the GDPR.

It applies directly to functions of Catholic University 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 Catholic University School.

3. Legal Obligations

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

- Under Section 9(g) of the Education Act, 1998, ensure that parent(s) / guardian(s) of a student, or in the case of a student who has reached the age of 18 years, the student, have access in the prescribed manner to records kept by that school relating to the progress of that student in 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 2014, as amended, 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 Child Protection Procedures for Primary and Post-Primary Schools 2017 published by the Department of Education and Skills, 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

Principle 1: Lawfulness, fairness and transparency
Catholic University 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. Advisory notices and privacy notices relating to data rights will be published as appropriate in plain English and will be structured where relevant to improve accessibility of this information to data subjects. Persons will be clearly advised of their rights also.

Principle 2: Purpose Limitation
Personal data collected by Catholic University 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 the change.

Principle 3: Data Minimisation
Catholic University 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 special category personal data.

Principle 4: Data Accuracy
Catholic University School will make every effort to ensure that subjects' information is accurate and up to date. Catholic University 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 Reception.

Principle 5: Storage Limitation
Catholic University School will store and retain personal data only while there is a valid and lawful basis to do so. Personal data 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 data fields with substituted generic text.

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. Catholic University School will use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability
Catholic University School is responsible for and is able to demonstrate compliance with GDPR. This means Catholic University School will demonstrate that these Data Protection Principles (as outlined here) are met for all Personal Data for which it is responsible.

5. Data Subject's Rights

Rights of Data Subjects
Catholic University 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.

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. This period may be extended by two further months, where necessary, taking into account the complexity and number of the requests.

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. Right of access requests must be responded to within one month. This period may be extended by two further months, where necessary, considering the complexity and number of the requests.

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 and Skills to provide future services to you or to meet it statutory obligations for example under the National Archives Act, 1986.

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, Catholic University School will carry out an assessment of whether the data can be restricted without affecting the ability of the School / Department of Education and Skills to provide future services to you.

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.

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.

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 which do 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.

6. Responsibilities – 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.

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

7. Responsibilities – Senior Management

- Ensure the policy is communicated to all relevant stakeholders.
- Ensure the policy is implemented throughout the school.
- Ensure personal data relating to students & staff is collected and processed in accordance with this policy.
- Ensure that the basic principles of data protection are explained to staff. This will be done during staff induction, staff meetings and other appropriate forums.
- Identifying training needs and arranging for refresher training sessions.
- 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.
- Escalating appropriate issues to the Board of Management.
- Taking appropriate preventative actions to mitigate the risk of data breaches arising.
- Leading the response to any data breach.
- Conduct due diligence of service providers (data processors) prior to any service provider being engaged. i.e. adequate assurances of GDPR.
- Ensuring appropriate written contracts in place with all service providers.
- Ensure that Record-keeping of data protection items is carried out.
- Ensure sensitive files and meeting minutes are held securely i.e. in locked filing cabinets or were held digitally encrypted.
- Ensure records that identify vulnerable persons or particularly sensitive data is anonymized / pseudonymized.
- When emailing minutes, documents will be password protected.
- Ensure that information is kept secure at all times and that the information is shredded as soon as could be reasonably expected.
- Periodic reviews of all data protection arrangements are carried out.

8. Responsibilities – Teachers

General

- Read and sign acknowledgement of this policy.
- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty.
- Check that any information that you provide in connection with their employment is accurate and up to date.
- Adherence to high standards of ethics and professionalism in all data entries (e.g. when entering notes about a student on any system).
- Ensure personal data is kept safe and secure, and is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party.
- Ensure personal data related to students is accurately processed in accordance with this policy.
- Ensure personal data (particularly special categories of personal data under Article 9 GDPR ("special category personal data") is never brought off-site unless appropriate steps are taken to protect the data in motion (e.g. if taking personal data to a TUSLA case conference to review a child, ensure the data are stored securely on an encrypted laptop).
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data.
- Assisting the Principal with access requests.

Handwritten Notes / Paper Records

- Handwritten Notes can be lost or mislaid (whether in a notebook or otherwise).
- Staff are urged to use the functionality provided on VS Ware and other school systems for securing records.
- Staff are advised of the following when taking records i.e. handwritten or otherwise:
    - If appropriate, the information on the note should be transferred to VS Ware, and the note shredded or,
    - Note is transferred to the central student file in the Principal PA's office or
    - If none of the above options are appropriate, then the note is destroyed / shredded as per the retention policy.
- Information required for Parent(s) / guardian(s) Teacher Meetings may be printed off VS Ware for that specific purpose providing that the teacher keeps that information secure at all times and that the information is shredded as soon as could be reasonably expected. Under no circumstances will teachers be permitted to take this information off the school premises.

Records

- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data.
- Ensure records are factual, non-judgemental and to the point.
- Only school supplied software is permitted for the recording of personal data at the school.

Electronic Records

- Personal data must be processed exclusively on school-supplied devices authorised for such purposes, and staff must refrain from using personal devices for handling personal data, i.e. Handling personal data involves activities such as collecting, storing, accessing, updating, sharing, protecting, responding to requests, and maintaining records.
- Should your school device get lost / stolen, staff will immediately notify the Principal who will then ensure that login details are reset.
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!).
- Ensure that personal data is not visible to others (e.g. never display VS Ware on a projector or leave your computer when logged into VS Ware).
- School servers / cloud have been provided to ensure availability of data, allowing appropriate back-ups to be made, ensuring accountability, transparency, as well as keeping data safe and secure, etc. Staff are urged to use this infrastructure.
- When working with personal data, all staff must ensure that the screens of their computers / tablets / apps are always locked when left unattended.
- Never storing personal data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.) and otherwise complying with the Staff Acceptable Use, IT & Mobile Devices Policy.

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 special category personal data, staff are required to encrypt these emails i.e. ensuring only those with a password can open and access the contents of the email.
- Encrypting emails where appropriate for other uses including the use of “Do Not Forward” etc.
- Attachments containing personal data should be downloaded, stored securely, and then deleted.
- Data should be encrypted before being transferred electronically.
- Staff will not save copies of personal data to their own computers, phones, tablets, USB sticks, Hard Drives.

Social Media

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

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 and / or appropriate
- Ensure passwords are unique (e.g. do not use the same password for your Social media account as for your VS Ware account etc).

9. Responsibilities – Administrators

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.
- Keeping Personal Data only as per the Retention Policy.
- Ensure data related to students, parent(s) / guardian(s) and staff is accurately processed in accordance with this policy.
- Establish and maintain a clean desk policy.
- 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 office.
- Ensure that their computer screen is not visible to visitors to the office.
- Diligence and attention-to-detail when entering data on to VS Ware or other systems and software.
- Keep the data accurate, complete, and up to date.
- Ensuring filing cabinets and office door is kept locked when not in use.
- Keep anti-virus and anti-malware software up to date as required.
- Respect access-permission levels, never looking into files/records to which you have no genuine reason for accessing.
- Prepare post with high levels of diligence and attention to detail. Ensuring that the correct letter is put in the correct envelope.
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data.

Subject Access Request

- Identify data subject access 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 to obtain the personal data.

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.

Phishing / Malware

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

10. Responsibilities – Year Heads

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

11. Responsibilities – AEN Department including 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 summary assessments for teaching staff).
- Take all reasonable measures to secure special category personal data 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 Student Support Plans are prepared, ensure that access to that document(s) is password protected to prevent unauthorised access.
- Ensure that the distribution of data relating to students' special education needs is done so securely and, on a needs know basis i.e. only teaching staff who teach a particular student.
- Limit identifying persons in emails / attachments where at all possible. Use of codes should be adopted where necessary.
- Where emails and attachments contain special category personal data, staff are required to encrypt the attachment to these emails i.e. ensuring only those with a password can open and access the contents of the email.
- Attachments containing personal data should be downloaded, stored securely, and then deleted.
- Staff will not save copies of personal data to their own computers, phones, tablets, USB sticks, Hard Drives.
- Ensuring that at all times the AEN Office & Filing Cabinets are locked when not in use.
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data.
- 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 central student file as soon as possible (to ensure availability of data, ensuring accountability, transparency, as well as keeping data safe and secure, etc).
- Assisting senior management in adhering to the school's retention schedule i.e. amalgamation of files relating to students in the central student file.
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.
- Ensure personal data (particularly special category personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop.
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!).
- Ensure passwords are unique (e.g. do not use the same password for your Social media account as for your school account etc).
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data.
- Assisting the Principal with subject access requests.

12. Responsibilities – Guidance Counsellor

- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty.
- Adherence to high standards of ethics and professionalism in all data entries i.e. notes and record keeping.
- Take all reasonable measures to secure personal data regarding students i.e. securing notes and records, ensuring your laptop or desktop computer is password protected and you log out each time you leave it.
- Use of codes to identify students in reports / files / relevant filing systems.
- Limit identifying persons in emails / attachments where at all possible. Adopting codes to identify students where necessary.
- Ensuring that the office and filing cabinets are locked when not in use.
- Where student files are online, ensure that documents are password protected to prevent unauthorised access.
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data.
- Where appropriate, ensure only relevant teachers are provided with personal data relating to a student.
- Ensure that any handwritten notes in any notebook are transferred to the central student file as soon as possible (to ensure availability of data, allowing appropriate back-ups to be made, ensuring accountability, transparency, as well as keeping data safe and secure, etc).
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.
- Ensure personal data is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop.
- Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.) and otherwise complying with the Staff Acceptable Use, IT & Mobile Devices Policy.
- 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!).
- Assisting senior management in adhering to the school's retention schedule i.e. amalgamation of files relating to students in the central student file.
- Ensure passwords are unique (e.g. do not use the same password for your social media account as for your school account etc).
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data.
- Assisting the Principal with subject access requests.

13. Responsibilities – Student Support Team

- Personal data must be processed exclusively on school-supplied devices authorised for such purposes, and staff must refrain from using personal devices for handling personal data, i.e. Handling personal data involves activities such as collecting, storing, accessing, updating, sharing, protecting, responding to requests, and maintaining records.
- Adhere to the values and standards set forth in this Policy and comply with relevant school procedures. Request clarification if there is uncertainty.
- Adherence to high standards of ethics and professionalism in all data entries.
- Take all reasonable measures to secure special category personal data regarding students i.e. securing notebooks and files in secure filing cabinets, ensuring your computer is password protected and you log out each time you leave it.
- Where minutes of meetings are prepared, ensure that access to that document(s) on the server / cloud is password protected to prevent unauthorised access.
- Use of codes to identify students in reports / files / relevant filing systems.
- Limit identifying persons in emails / attachments where at all possible. Adopting codes to identify students where necessary.
- Where emails and attachments contain special category personal data, staff are required to encrypt the attachment to these emails i.e. ensuring only those with a password can open and access the contents of the email.
- Attachments containing personal data should be downloaded, stored securely, and then deleted.
- Staff will not save copies of personal data to their own computers, phones, tablets, USB sticks, Hard Drives.
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data i.e. be factual, non-judgemental and to the point when preparing all records.
- Ensure only relevant teachers are provided with access to special category personal data relating to a student – be discreet and to the point.
- Ensure that any handwritten notes in any notebook are transferred to the central student file as soon as possible (to ensure availability of data, ensuring accountability, transparency, as well as keeping data safe and secure, etc).
- Ensure personal data (particularly special category personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop.
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!).
- Ensure passwords are unique (e.g. do not use the same password for your Social media account as for your school account etc).
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data.
- Assisting the Principal with subject access requests.

14. Responsibilities – Contractors, Maintenance Teams etc.

- 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.

15. Responsibilities – Data Processors etc.

- 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.

16. GDPR Awareness

Catholic University 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:

- GDPR Workshops with key staff.
- GDPR Briefing to all staff.
- A general email to all staff with the Data Protection Policy.

17. 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.

18. Data Protection Impact Assessments

Catholic University 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.

19. Lawful Processing Criteria

Catholic University 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 Processing Map & Retention Schedule.

20. Storage & Processing 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 Catholic University School. Appropriate security measures will be taken by the school to protect unauthorised access to this data and to the data it is processing 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.
- Paper files will be held centrally and stored in a relevant filing system, located away from public areas in locked cabinets.
- Computerised data will be held under password protected files.
- Any information which needs to be disposed of will be done so carefully and thoroughly.
- The premises at Catholic University School are protected by a private security company and is monitored on a 24 hour / 7-day week basis.

Paper based records
Paper based records shall not 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 centrally in a locked secured filing cabinet.
- VS Ware will be used for the purposes centralising digital records relating to students.
- Data will be shredded and disposed of securely.

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

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

Processing of Student Personal Data
As defined in Article 4 of the GDPR, "processing" means: "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

We process student's personal data for purposes including:

- Their application for enrolment.
- To provide them with appropriate education and support.
- To monitor their academic progress.
- To care for their health and well-being.
- To care for our staff and students.
- To process grant applications, payments and scholarships.
- To coordinate, evaluate, fund and organise educational programmes.
- To coordinate, evaluate, fund and organise school and extra-curricular activities and events.
- To create a pictorial and historical record of life, activities and events at the school.
- To comply with our legal obligations as an education body.
- To comply with our monitoring and reporting obligations to government bodies.
- To process student disciplinary procedures under Catholic University School code of behaviour and disciplinary procedures, appeals, resolve disputes, and defend litigation etc.
- For the safety of our staff and students and for the protection of personal and school property (including the use of CCTV and video recording).
- For the safety, health & wellbeing of other staff, students and visitors.

Use of Staff Personal Data
We use staff personal data for purposes including:

- Their application for employment.
- To provide them with appropriate direction and support in your employment.
- To care for their health and well-being.
- To care for our staff and students.
- To process grant applications, payments and scholarships.
- To coordinate, evaluate, fund and organise educational programmes.
- To coordinate, evaluate, fund and organise school and extra-curricular activities and events.
- To create a pictorial and historical record of life, activities and events at the school.
- 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 of our staff and students and for the protection of personal and school property (including the use of CCTV and video recording).
- For the safety, health & wellbeing of other staff, students and visitors.

Catholic University 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.

21. Sharing Personal Data

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

The sharing of personal data and the nature of what is shared depends on various factors. The Government bodies to which we transfer personal data will use that data for their own purposes (including: to verify other information they already hold etc.) and they may aggregate it with other information they already hold about the data subject and the data subject's family.

We also share personal data with other third parties including our insurance company and other service providers (including External Psychologists, Speech Therapists, IT providers, security providers, legal advisors etc.). We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parent(s) / guardian(s), including results of examinations.

22. Special Categories of Personal Data – Students / Prospective Students

Special categories of particularly sensitive personal data require higher levels of protection. The school through the Department of Education and Skills may:

- Collect information on ethnic/cultural background of students with the consent of the parent(s) / guardian(s) 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(s) / guardian(s) 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 and Skills will only process special categories of personal data relating to children or students for the purposes of allocating resources where this is provided for by way of enactment or the Constitution.

23. Special Categories of Personal Data – Staff

Special categories of particularly sensitive personal data require higher levels of protection. The school through the Department of Education and Skills 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.

24. Photographs and video

Our school often takes photographs (photos) and/or video recordings at school and extra-curricular activities and events to capture important occasions, and to evaluate those activities/events and to ensure the safety, health and wellbeing of all students, staff, visitors and property. These photos and/or videos are taken using cameras (including cameras on digital devices), by a member of staff or a post-holder(s) whose post includes photography/videography (e.g., the marketing team) or by a student under their direction, or by an external photographer/videographer contracted by the school.

In these scenarios, we are acting as data controllers under the GDPR and all of the obligations that come with it. For example, we must have a legal basis to process the personal data for the relevant purpose (e.g. take, store and use photos) and we must provide clear and concise information about this to the relevant data subjects, and how long we will be keeping it for.

1. Recording School life generally
It has become customary to take photos and/or videos of students & staff engaged in school and extra-curricular activities and events in the interest of creating a pictorial as well as historical record of life at the school. Our school maintains a database of such photos and videos from activities and events held over the years. For example, class and sports team photos, school shows and school trips. Photos and/or videos of students captured at these activities and events, and in some cases their names, may be published on our school website, app, on social media or in brochures, yearbooks, newsletters, local and national news media and similar school-related publications.

Consent
To lawfully process student personal data for this purpose, we rely on consent. Consent is requested from each parent(s) / guardian(s) using our consent letter. Should the parent(s) / guardian(s) wish to have his/her child's photo or video removed from the school website, brochure, yearbooks, newsletters etc. at any time, we will duly comply on receipt of a written request to the Principal. Please note that any photos or videos published by the school in yearbooks, newsletters, papers etc. up to this date, will remain in place based on previous consent given. No further photos/videos will be published after the date of revocation.

We do not overlook children and young people themselves in these scenarios. They also have rights in relation to their personal data and they will be made aware of the fact that their images are being taken and used, for example, in the local newspaper. As we do rely on consent as our legal basis, then the age of students intended to be photographed or video-recorded should be taken into account when it comes to seeking consent as students may be capable of making that decision for themselves. For example, the parent(s) / guardian(s) of a 15-year-old may have given consent for photographs or videos to be taken of their child at the school's show for publication in the local newspaper - however, the 15-year-old may very well have objections to this and may not wish to appear in the local newspaper.

We acknowledge each student's understanding of what exactly it is they are agreeing to and giving consent themselves. As such, depending on the context and the age of the student, it may be a case of involving both the parent(s) / guardian(s) *and* the student in the discussion about consent.

No Consent List
A list of students for whom consent has not been given for photos and/or videos to be taken and published/posted for this 'Record of School Life' purpose will be maintained by a committee made up of teachers, post holder(s) and management responsible for Data Protection. This list will be referred to on an ongoing basis to ensure that student photos and/or videos for this purpose are never published or posted without consent.

Posting & Publication
As noted above, where consent is received, photos and/or videos of students for this 'Record of School Life' purpose, and in some cases their names, may be published on our school website, app, on social media or in brochures, yearbooks, newsletters, local and national news media and similar school-related publications. The person taking these photos and/or videos must maintain the highest standards of privacy at all times.

Those posting these photos and/or videos shall ensure that the use of the photo and/or video is consistent with the explanation of use for this 'Record of School Life' purpose as requested using our consent form.

In post-production / pre-posting on social media, website etc. those posting will in good faith, take into consideration compromising photos/videos i.e. facial expressions, gestures or other physical postures which may cause the subject of the photo/video (or those in the background) undue stress and concern. In these scenarios, these photos/videos will not be posted and will also be deleted from the One Drive permanently.

Local & National News media
Once consent is received, then the sharing of photos/videos for this 'Record of School Life' purpose with local and national news media will be facilitated by the school.

2. Recording specific School activities and events

Our school also takes photos and/or video recordings (including CCTV recordings) of specific school and extracurricular activities and events, such as sports matches and school trips. This is for the purposes of evaluating and/or monitoring those activities/events and ensuring the safety, health and wellbeing of all students, staff, visitors and property. For example, video recordings of school sports matches facilitate evaluation of team performance and coaching. In addition, if any alleged student disciplinary matters arise at these activities/events, the relevant photos and/or video/CCTV recordings may also be used in any subsequent student disciplinary proceedings arising.

Legitimate interests
To lawfully process student personal data for this purpose, the school does not rely on consent. Instead, the school considers that this processing is necessary for the purpose of its legitimate interests in evaluating and/or monitoring school and extracurricular activities and events and ensuring the safety, health and wellbeing of all students, staff, visitors and property. In particular, having carried out a legitimate interest balancing exercise, the school is satisfied that its legitimate interests are not overridden by the interests or fundamental rights and freedoms of the students in this regard.

Household Exemption
Occasionally students and/or families taking photos and/or videos at school and/or extracurricular activities and events are simply doing so for reminiscence's sake and don't intend to post or publish the photos anywhere. This type of activity falls under the so-called "household exemption" under the GDPR. This provides that the GDPR does not apply when a person processes personal data (for example, a photo of someone) in the course of a purely personal or household activity, e.g. with no connection to a professional, business, official or commercial activity.

It's important to note that in this context, we are in a very different position to parent(s) / guardian(s) / family / friends in that we cannot rely on the household exemption.

School cameras and equipment
Where members of staff or students under their direction take photos and/or video recordings at a school or extracurricular activity/event, this will be done using the school supplied equipment and subject to the Staff Acceptable Use, IT & Mobile Devices Policy. In this scenario, photos/videos taken on the app should be saved to the school supplied Microsoft 365 and not on the teacher's own personal camera roll on their phone.

CCTV recordings will comply with the school's CCTV Policy.

Storage
Photos and videos of students will be saved on the school's Microsoft 365. This account will be accessible by a committee made up of teachers, post holder(s) and management. Appropriate measures will be taken to ensure that this has appropriate storage capability (up to 1 TB) and access control.

Access
Access to photos and videos will be restricted to appropriate teachers, relevant post holder(s) and management and the downloading of these images on to personal storage devices is prohibited.

Account usernames & passwords for websites, social media accounts etc. will be centrally stored and available to the committee and senior management to administer and control the use of photos and videos in accordance with this policy.

25. Data Processing Map & Retention Schedule

Everyone who works for Catholic University School has a responsibility for ensuring data is organised, secured, and retained appropriately. Each person who handles personal data must ensure that it is processed in line with this policy and the data protection principles.

Personal Data processed at Catholic University School is summarised in the Data Processing Map along with our legal justification for processing this data and our Retention Policy for same.

Data Processing 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.

26. 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 **Microsoft 365**	Restricted	Microsoft 365 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.	Standard Contractual Clauses	Indefinitely.	N/a	**Technical:** Individual Logins for Staff. Authentication by 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. **Organisational:** Relevant employees trained on GDPR awareness.
D02 **VS Ware**	Confidential	Cloud: VS Ware	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Student Data incl. Name. Surname. Date of Birth. PPS Number. Address. Parent(s) / guardian(s) Name. Parent(s) / guardian(s) Phone Number. Parent(s) / guardian(s)Guardian Home address, Mobile, Emergency Contact Person & No., Email, Nationality, Birth Certificate, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History. Academic Progress.	Administrators. Teachers. Deputy Principal. Principal.	N/a	Up to 7 years after the student finishes / would have finished 6th Year (or sooner at School's discretion).	N/a	**Technical:** Individual Logins for Staff. Authentication by VS Ware System using username and password. Admin Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Behaviour, Discipline, Docs, Notes, AEN , Classes & Groups, Medical, Account, Enrolment History. Teacher Permissions: (Limited access). Roll Call (AM/PM). Teachers Timetable. Absent without Leave. Assessment (Exams on system). Access to students they teach in a particular class. VS Ware uses SSL/TLS protocol that provides secure communications for accessing and updating the record. **Organisational:** Data Processing Agreement in place with VS Ware. 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
D03 CCTV	Restricted	Principal's Office.	Crime-prevention, the prevention of anti-social behaviour, the prevention of bullying, the safety of our staff and students and the protection of personal and school property.	Public Interest.	Video & Images.	Principal. Deputy Principal. Contractors.	N/a	28 Days.	N/a	**Technical:** Images are retained for 28 Days Maximum. Internal 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. **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.
D04 Photographs	Restricted to authorised to specific publishing mediums i.e. school website, social media etc.	On devices taking photos. Walls of School. Website & Social Media Channels, Newsletters, Newspapers.	Documenting, promoting or celebrating through press coverage, websites, prospectuses etc.	Consent.	Images.	Anyone visiting our school, social media channels, website.	N/a	Indefinitely. Pending Review by the BoM.	N/a	**Technical:** 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 photographs posted to the website / social media. Consent sought from Parents / Guardians. For any photographs/video recordings subsequently used for the purposes of a disciplinary procedure. **Organisational:** Staff briefed on the Data Protection Policy.
D05 Classroom Based Assessments	Restricted	School Devices.	CBA Videos assess research and communication / presentation skills of Junior Cycle Students. Learning Logs are used in TY for similar purposes.	Legal Obligation.	Video.	Teachers.	N/a	Assessment Period.	Deleted from Hard Drive of School Device.	**Technical:** School devices are only permitted for the recording of classroom based assessments and learning logs. Recordings are only kept for the period required to assess the student's work. Once assessment & SLAR Meeting has taken place and the results documented, then the recording will be deleted from the device. Assessment period is no longer than 1 month. **Organisational:** Staff briefed on the Data Protection Policy.
D08 Social Media	Public	Social Media Provider Servers	Provide information to students, parent(s) / guardian(s) and staff.	Public Interest.	Personal Data incl. Photos of Academic Achievement Awards, Staff Retirements etc.	Public.	Standard Contractual Clauses.	Until we delete our School Instagram Account.	N/a	**Technical:** Individual Logins for Account Administrator. Authentication using username and password. Administrator has full rights to remove photos and posts from the Account if needed. **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
D09 **Local Server**	Restricted	Main Office.	Local File Storage.	Public Interest. Legal Obligation.	Personal Data incl. Student Data, Staff Data, Policies & Procedures.	Administrators. IT Support. Teachers. Deputy Principal. Principal.	N/a.	Indefinitely. Pending Review by the BoM.	N/a	**Technical:** Individual Logins for Staff. IT Support has full rights to the network. HEA Net provide robust external network firewalls. Internal Firewall in place (Windows). Back-ups carried out once per month. **Organisational:** Comms Cabinets locked at all times. Data Processing Agreement in place with IT Company. Relevant staff trained on The Data Protection Policy.
D010 **Website**	Confidential	Google	Provide information to students, parent(s) / Guardian(s) and staff.	Public Interest. Legal Obligation.	Personal Data incl. Photos of Academic Achievement Awards, Staff Retirements etc.	Parent(s) / Guardian(s) of Students. Administrators. Teachers. Deputy Principal. 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.

27. 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
D011 **Registers & Roll Books**	Confidential	**Cloud:** VS Ware **Paper:** Main Office	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(s) / guardian(s) Name. Parent(s) / guardian(s) Phone Number. Parent(s) / guardian(s) Home address, Mobile, Emergency Contact Person & No., Email, Nationality, Birth Certificate, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History. Photos.	Administrators. Teachers. Year Heads. Deputy Principal. Principal. Parents / guardians.	N/a	Indefinitely. Archive when class leaves + 2 years.	N/a	**Technical:** Individual Logins for Staff. Authentication by VS Ware System using username and password. Admin Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Behaviour, Discipline, Docs, Notes, AEN , Classes & Groups, Medical, Account, Enrolment History. Teacher Permissions: (Limited access). Roll Call (AM/PM). Teachers Timetable. Absent without Leave. Assessment (Exams on system). Access to students they teach in a particular class. VS Ware uses SSL/TLS protocol that provides secure communications for accessing and updating the record. **Organisational:** Office is locked when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Computers on which records are accessible are password protected and are accessible only to designated staff. Staff briefed on the Data Protection Policy.
D012 **State Exam Results**	Confidential	**Originals:** Dept of Education. **Cloud:** VS Ware **Paper:** Main Office.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Administrators. Teachers. Deputy Principal. Principal.	N/a	Up to 7 years after the student finishes 6th Year. Following this the student can make an application to the Dept.	Confidential Shredding.	**Technical:** Individual Logins for Staff. Authentication by VS Ware System using username and password. Admin Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Behaviour, Discipline, Docs, Notes, AEN , Classes & Groups, Medical, Account, Enrolment History. Teacher Permissions: (Limited access). Roll Call (AM/PM). Teachers Timetable. Absent without Leave. Assessment (Exams on system). Access to students they teach in a particular class. VS Ware uses SSL/TLS protocol that provides secure communications for accessing and updating the record. **Organisational:** Staff permitted to access results of students in their class. 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
D013 Application / Enrolment Forms	Confidential	**Paper:** Main Office. **Electronic:** P-Pods. VS Ware.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Student Data incl. Name. Surname. Date of Birth. PPS Number. Address. Parent(s) / guardian(s) Name. Parent(s) / guardian(s) Phone Number. Parent(s) / guardian(s) Home address, Mobile, Emergency Contact Person & No., Email, Nationality, Birth Certificate, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History. Photos.	Administrators. Year Heads. Principal. Deputy Principal.	N/a	Up to 7 years after the student finishes / would have finished 6th Year (or sooner at School's discretion). Those students not enrolling 12 months after registration closing date.	**Paper Copies:** Confidential shredding. **VS Ware:** Securely Delete Student Profile.	**Technical:** Individual Logins for Staff. Authentication by VS Ware System using username and password. Admin Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Behaviour, Discipline, Docs, Notes, AEN, Classes & Groups, Medical, Account, Enrolment History. Teacher Permissions: (Limited access). Roll Call (AM/PM). Teachers Timetable. Absent without Leave. Assessment (Exams on system). Access to students they teach in a particular class. VS Ware uses SSL/TLS protocol that provides secure communications for accessing and updating the record. **Organisational:** Office Locked when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Computers on which records are stored are password protected and are accessible only to designated staff. Admin trained on the admin of the P-Pod & VS Ware software. Staff briefed on the Data Protection Policy.
D014 Disciplinary Notes	Confidential	**Electronic:** VS Ware. **Paper:** Locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data. Incl. Student Name. Class. Teacher. Description of Problem. Frequency of Behaviour. Intervention made to date. Student Reaction to Teacher / Year Head.	Principal. Deputy Principal. Year Head. Teachers. Parents / Guardians.	N/a	Significant Cases – Indefinitely but reviewed annually. All other records Up to 7 years after the student finishes / would have finished 6th Year (or sooner at School's discretion).	**Paper Copies:** Never Destroy.	**Technical:** Individual Logins for Staff. Authentication by VS Ware System using username and password. Admin Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Behaviour, Discipline, Docs, Notes, AEN, Classes & Groups, Medical, Account, Enrolment History. Teacher Permissions: (Limited access). Roll Call (AM/PM). Teachers Timetable. Absent without Leave. Assessment (Exams on system). Access to students they teach in a particular class. VS Ware uses SSL/TLS protocol that provides secure communications for accessing and updating the record. **Organisational:** Only designated Year Heads & Senior Management have access to this information. Filing cabinets holding these records will be locked at the end of each day. Relevant employees briefed on the Data Protection Policy and the AEN Policy. Office is locked when not in use.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D015 **Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results).**	Confidential	**Electronic:** VS Ware	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Administrators. Principal. Deputy Principal. Year Head. Parents / Guardians.	N/a	Up to 7 years after the student finishes / would have finished 6th Year (or sooner at School's discretion).	**Paper Copies:** Confidential shredding.	**Technical:** Authentication by VS Ware System using username and password. Main Office Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Payments, Behaviour, Discipline, Docs, Notes, AEN, Classes & Groups, Medical, Account, Enrolment History. VS Ware use SSL/TLS protocol that provides secure communications for accessing and updating the record. Electronic Records are backed up periodically. **Organisational:** Offices are locked when not in use. Computers logged out when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Staff briefed on the Data Protection Policy.
D016 **End of term/year reports**	Confidential	**Electronic:** VS Ware	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Administrators. Principal. Deputy Principal. Year Head. Parents / Guardians.	N/a	Up to 7 years after the student finishes / would have finished 6th Year (or sooner at School's discretion).	**Paper Copies:** Confidential shredding.	**Technical:** Authentication by VS Ware System using username and password. Main Office Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Payments, Behaviour, Discipline, Docs, Notes, AEN, Classes & Groups, Medical, Account, Enrolment History. VS Ware use SSL/TLS protocol that provides secure communications for accessing and updating the record. Electronic Records are backed up periodically. **Organisational:** Offices are locked when not in use. Computers logged out when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D017 **Absences**	Confidential	**Electronic:** VS Ware	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data.	Administrators. Principal. Deputy Principal. Year Heads. Parents / Guardians. Tusla.	N/a	Up to 7 years after the student finishes / would have finished 6th Year (or sooner at School's discretion).	**Paper Copies:** Confidential Shredding.	**Technical:** Authentication by VS Ware System using username and password. Main Office Staff / Principal / Deputy Principal: Permission (Full Admin Rights): Student Profiles: Personal (Application Form), Household, Attendance, Term Reports, Timetable, Payments, Behaviour, Discipline, Docs, Notes, AEN, Classes & Groups, Medical, Account, Enrolment History. VS Ware use SSL/TLS protocol that provides secure communications for accessing and updating the record. Electronic Records are backed up periodically. **Organisational:** Offices are locked when not in use. Computers logged out when not in use. Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Staff briefed on the Data Protection Policy.
D018 **Records of school tours/trips, including permission slips, itinerary reports.**	Confidential	**Paper:** Teacher Organising the Trip to provide these to the Deputy Principal's Office. Stored in locked and secure filing cabinets.	Fulfil processing of student records in the course of organising a school trip.	Public Interest. Legal Obligation.	Personal Data incl. Consent Forms.	Principal. Deputy Principal. Teachers. Tusla.	N/a	**Overnight Trips:** Up to 7 years after the student finishes / would have finished 6th Year (or sooner at School's discretion). **Day Trips:** 1 Month after the trip on condition that no accidents / incidents were reported.	**Day Trip Paper Copies:** Confidential Shredding.	**Technical:** Minimal Data including consent collected from the parent(s) / guardian(s) in order to book the trip. In some cases, when school trips are taken abroad student's will be asked to provide necessary information to a travel agent directly i.e. Name, Address, DOB, Passport Number where Data Processing Agreement is in place. **Organisational:** Copies of consent forms kept on file with teacher. Computers on which records are stored are password protected and are accessible only to designated staff.
D019 **Garda vetting form & outcome – STUDENTS**	Confidential	**Paper:** Principal's Office.	Fulfil processing of student records in the course of gaining work experience.	Public Interest. Legal Obligation.	Personal Data.	Placement Employer. Administrators. Teachers. Deputy Principal. Principal.	N/a	Record of outcome retained for 12 months.	**Paper Copies:** Confidential shredding.	**Technical:** Only processed for those over 16 years of age with the consent of a parent(s) / guardian(s). **Organisational:** School to retain the reference number and date of disclosure on file, which can be checked with An Garda Siochana in the future. Computers on which records are stored are password protected and are accessible only to designated staff.

28. Sensitive Personal Data

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 Psychological assessments	Confidential	**Paper:** AEN Office.	Fulfil processing of student records in the course of delivering education.	Legal Obligation.	Personal Data incl. Name. Surname. Results of Psychological Assessment.	AEN Coordinator. Additional Education Teachers. Administrators. Year Head. Deputy Principal. Principal.	N/a	Indefinitely but reviewed annually.	**Paper Copies:** Never Destroy.	**Technical:** AEN Coordinator, SNAs & Senior Management have access to this information. Filing cabinet located in locked office. **Organisational:** Filing cabinets holding these records will be locked at the end of each day. Relevant employees briefed on the Data Protection Policy and the AEN Policy. Office is locked when not in use.
D021 Additional Education Needs' files, reviews, correspondence and Student Support Plans	Confidential	**Paper:** AEN Office.	Fulfil processing of student records in the course of delivering education.	Legal Obligation.	Personal Data incl. Name. Surname. Results of Psychological Assessment. Reviews, correspondence and Student Support Plans.	AEN Coordinator. Additional Education Teachers. Administrators. Year Head. Deputy Principal. Principal.	N/a	Indefinitely but reviewed annually.	**Paper Copies:** Never Destroy.	**Technical:** Only designated Staff & Senior Management have access to this information. **Organisational:** Filing cabinets holding these records will be locked at the end of each day. Relevant staff briefed on the Data Protection Policy and the AEN Policy. Office is locked when not in use.
D022 Student Support Plans	Restricted	**Paper:** AEN Office.	Fulfil processing of student records in the course of delivering education.	Legal Obligation.	Personal Data incl. Name. Surname. Results of Psychological Assessment. Reviews, correspondence and Student Support Plans.	AEN Coordinator. Additional Education Teachers. Administrators. Year Head. Timetabled Teachers. Inspector. Deputy Principal. Principal. Parents / Guardians.	On server.	Indefinitely but reviewed annually.	**Paper Copies:** Never Destroy.	**Technical:** Access to server restricted. External IT company maintaining the server and security. Only designated Additional Education Teachers, Class Teachers & Senior Management have access to this information. AEN Filing cabinet located in locked office. **Organisational:** Filing cabinets holding these records will be locked at the end of each day. Relevant employees briefed on the Data Protection Policy and the AEN Policy. Office is locked when not in use.
D023 Guidance Counselling Records	Confidential	**Paper:** Student's File with Guidance Counsellor in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Legal Obligation.	Personal Data incl. Sensitive Personal Details.	Guidance Counsellor. External Counsellor.	N/a	Indefinitely but reviewed annually.	**Paper Copies:** Never Destroy.	**Technical:** Data Processing Agreement in place with external counsellor. **Organisational:** Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. 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
D024 DAT	Confidential	**Paper:** Student's File with Guidance Counsellor in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Legal Obligation.	Personal Data incl. Sensitive Personal Details.	Guidance Counsellor. CAT 4 Providers. In certain circumstances the appropriate people/agencies or authorities may be informed. The students are made aware of these conditions. Timetabled Teachers. Deputy Principal. Principal. Parents / Guardians.	N/a	Indefinitely but reviewed annually.	**Paper Copies:** Never Destroy.	**Organisational:** Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Relevant staff briefed on the Data Protection Policy.
D025 Child Protection Records D026	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil our legal obligation under Child Protection Procedures for Primary and Post-Primary Schools 2017.	Legal Obligation.	Personal Data.	Principal (Designated Liaison Person). Deputy Principal (Deputy Designated Liaison Person). Board of Management.	N/a	Indefinitely but reviewed annually.	**Paper Copies:** Never Destroy.	**Technical:** All incidents are reported to the Principal (Designated Liaison Person) as per the Child Safeguarding Statement of the school. Principal's Office is locked when not in use. **Organisational:** Relevant staff briefed on the Data Protection Policy and the Child Safeguarding Statement.
D027 Section 29 appeal records	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Legal Obligation.	Personal Data incl. Name. Surname. Address, Home Tel. Number. Daytime Tel. Number. Mobile Tel. Number. Date of Birth. Year / Class of Student. AEN Requirement. Nature of Decision. Particulars associated with the expulsion.	Principal. Board of Management.	N/a	Indefinitely but reviewed annually.	**Paper Copies:** Confidential Shredding.	**Technical:** All appeal records are reported to the Board of Management as per the Admissions Policy of the school. These records will be held in the Principal's Office which is locked when not in use. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D028 Incoming 1st Year Student Information	Confidential	**Electronic:** Microsoft 365	Fulfil processing of student records in the course of delivering education.	Legal Obligation.	Personal Data incl. Name. Surname. Address, Home Tel. Number. Daytime Tel. Number. Mobile Tel. Number. Date of Birth. Year / Class of Student. AEN Requirement. Nature of Decision. Particulars associated with the expulsion.	Principal. Board of Management.	N/a	Up to 7 years after the student finishes / would have finished 6th Year (or sooner at School's discretion).	Deletion	**Technical:** Individual Logins for Staff. Authentication by 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. **Organisational:** Relevant employees trained on GDPR awareness.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D029 **Accident Reports**	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil processing of student records in the course of delivering education.	Public Interest. Legal Obligation.	Personal Data incl. Name. Surname. Address, Particulars associated with an incident.	Principal (Designated Liaison Person). Deputy Principal (Deputy Designated Liaison Person). Board of Management. Administrators. State Claims Agency. Insurance Company.	N/a	10 Years.	**Paper Copies:** Confidential Shredding.	**Technical:** Individual Logins for Staff. Authentication by G-Suite for Education 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. **Organisational:** All incidents are reported to the Principal (Designated Liaison Person) as per the Child Safeguarding Statement of the school. Principal's Office is locked when not in use. Relevant staff briefed on the Data Protection Policy and the Health & Safety Policy.
D030 **Enrolment /transfer forms where child is not enrolled or refused enrolment**	Confidential	**Paper:** Main Office in locked and secure filing cabinets.	Fulfil processing of student records in the normal course of school operations.	Legal Obligation.	Student Data incl. Name. Surname. Date of Birth. PPS Number. Address. Parent(s) / guardian(s) Name. Parent(s) / guardian(s) Phone Number. Parent(s) / guardian(s) Home address, Mobile, Emergency Contact Person & No., Email, Nationality, Birth Certificate, Mothers Maiden Name, Family Members (current / past), Medical Card, Medical Conditions, Name, Address & Tel. No. of GP, Previous Educational History	Administrators. Principal. Deputy Principal.	N/a	12 Months.	**Paper Copies:** Confidential Shredding. **VS Ware:** Securely Delete Student Profile.	**Technical:** Individual Logins for Administrators. Authentication by Esinet P-Pods System using username and password. P-Pods use SSL/TLS protocol that provides secure comms 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 Esinet software. Filing cabinets locked and secured when not in use. Staff briefed on the Data Protection Policy.
D031 **Records of complaints made by parent(s) / guardian(s) / students**	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. Deputy Principal. Those the subject of the complaint.	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. Otherwise Up to 7 years after the student finishes 6th Year. Confidential Shredding.	**Technical:** Paper records are filed and stored in secure locked cabinets to which only designated staff have access. Principal's Office is locked when not in use. **Organisational:** Staff briefed on the Data Protection Policy.

29. 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
D032 Applications & CVs of candidates called for interview **D033 Database of applications** **D034 Selection Criteria** **D035 Applications of candidates not shortlisted** **D036 Unsolicited job applications** **D037 Candidates shortlisted but not successful** **D038 Interview board marking scheme and notes** **D039 Panel recommendation**	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets. **Electronic:** School email.	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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	**Unsuccessful Candidate:** 18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken. **Successful Candidate:** Retain for duration of employment plus 7 years.	**Paper Copies:** Confidential Shredding. **Electronic:** Delete email.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

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

30. 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
D040 Applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, training etc.	Confidential	**Paper:** Teacher's File 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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years.	**Paper Copies:** Confidential Shredding. **Electronic:** Delete Staff Profile.	**Technical:** Electronic Records are backed up periodically. **Organisational:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff.
D041 Application &/CV										
D042 Qualifications										
D043 References										
D044 Interview: database of applications (the section which relates to the employee only)										
D045 Selection Criteria										
D046 Interview Board Marking Scheme & Boards Notes										
D047 Panel recommendation by interview board										
D048 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
D049 Job Specification / Description **D050 Contract/ Conditions of employment** **D051 Probation letters/forms** **D052 POR applications & correspondence (whether successful or not)** **D053 Leave of absence applications** **D054 Job Share** **D055 Career Break**	Confidential	**Paper:** Teacher's File 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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Computers on which records are stored are password protected and are accessible only to designated staff. Electronic Records are backed up periodically. **Organisational:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day.
D056 Maternity / Paternity Leave	Confidential	**Paper:** Teacher's File in Principal's Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for 2 years following retirement /resignation or the duration of employment plus 7 years (whichever is the greater).	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by Esinet system using user-name and password. Esinet use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D057 Parental Leave	Confidential	**Paper:** Teacher's File in Principal's Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Must be kept for 8 years - Parental Leave Act 1998 Retain for 8 years or the duration of employment plus 7 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by Esinet System using user-name and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D058 **Force Majeure Leave**	Confidential	**Paper:** Teacher's File in Principal's Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for 8 years or the duration of employment plus 7 years (whichever is the greater). There is a statutory requirement to retain for 8 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by Esinet System using user-name and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D059 **Carer's Leave**	Confidential	**Paper:** Teacher's File in Principal's Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Must be kept for 8 years - Carer's Leave Act 2001 Retain for 8 years or the duration of employment plus 7 years (whichever is the greater).	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by Esinet system using user-name and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D060 **Working Time Act (attendance hours, holidays, breaks)**	Confidential	**Paper:** Teacher's File in Principal's Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Authentication by Esinet System using user-name and password. P-Pods use SSL/TLS protocol that provides secure communications for accessing and updating the record. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D061 Allegations / Complaints relating to a member of staff (made by management, a colleague, student, parent(s) / guardian(s).	Confidential	**Paper:** Teacher's File 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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal. Those the subject of the complaint.	N/a	Retain for duration of employment plus 7 years Please note the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D062 Grievance and Disciplinary records	Confidential	**Paper:** Teacher's File 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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal. Board of Management.	N/a	Retain for duration of employment plus 7 years Please note the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

31. 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
D063 Sickness Absence Records / Certificates **D064 Pre-Employment Medical Assessment** **D065 Occupational Health Referral** **D066 Correspondence regarding retirement on ill-health grounds**	Confidential	**Paper:** Teacher's File in Principal's Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for 7 years unless sickness absence relates to an accident / injury / incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.	**Paper Copies:** Confidential Shredding unless sickness absence relates to an accident / injury / incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Individual Logins for OLCS. Esinet System authenticates using username and password. Esinet 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 ESINET system. Staff briefed on the Data Protection Policy.
D067 Accident / Injury at Work Reports	Confidential	**Paper:** Teacher's File in Main Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Indefinitely. Pending Review by the BoM.	Do not destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D068 **Medical assessments or referrals regarding fitness for work**	Confidential	**Paper:** Teacher's File in Principal's Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years There is a statutory requirement to retain for 3 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Relevant staff briefed on the Data Protection Policy.
D069 **Sick Leave Records (Sick Benefit Forms)**	Confidential	**Paper:** Teacher's File in Principal's Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Retain for duration of employment plus 7 years There is a statutory requirement to retain for 3 years.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Individual Logins for OCLS. Esinet System authenticates using username and password. Esinet 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 ESINET system. Staff briefed on the Data Protection Policy.

32. 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
D070 **Records of previous service (incl. correspondence with previous employers)**	Confidential	**Paper:** Finance Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Indefinitely. Pending Review by the BoM.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D071 **Pension Calculation**	Confidential	**Paper:** Finance Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Indefinitely. Pending Review by the BoM.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D072 **Pension increases**	Confidential	**Paper:** Finance Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Duration of employment + 7 years or for the life of employee/ former employee plus + 7 years - whichever is the longer.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D073 **Salary Claim Forms**	Confidential	**Paper:** Finance Office in locked and secure filing cabinets. **Electronic:** Esinet	HR activities of the school.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Duration of employment + 7 years or for the life of employee/ former employee plus + 7 years - whichever is the longer.	**Paper Copies:** Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.

33. Government Returns

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D074 **Any returns which identify individual staff/pupils.**	Confidential	**Paper:** Main Office in locked and secure filing cabinets. **Electronic:** VS Ware	Fulfil processing of student records in the normal admin of school operations.	Public Interest. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal. Teachers.	N/a	Depends upon the nature of the return. If it relates to pay/pension / benefits of staff, keep indefinitely as per DES guidelines. If it relates to information on students, e.g. October Returns, Annual Census etc., keep in line with "Student Records" guidelines above.	**Paper Copies:** Confidential Shredding.	**Technical:** Authentication by VS Ware System using username and password. Main Office Staff / Principal / Deputy Principal: Permission (Full Admin Rights): VS Ware use SSL/TLS protocol that provides secure communications for accessing and updating the record. Electronic Records are backed up periodically. Computers are password protected and are only accessible by designated staff. **Organisational:** Only the minimum data is collected from the data subject to fulfil our processing needs. Office is locked when not in use. Staff briefed on the Data Protection Policy.

34. 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
D075 **Board agenda and minutes**	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Fulfil good governance and running of the school in the Public Interest.	Public Interest. Defence of Legal Claim.	Student Personal Data. Staff Personal Data.	Board of Management. Principal. Deputy Principal.	N/a	Indefinitely.	Do Not Destroy	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Desktop computer is encrypted. Office is locked when not in use. **Organisational:** BOM Minutes and records are kept secure in locked filing cabinets at all times. Electronic versions of BOM Minutes are kept secure in password protected folders. Minutes that identify vulnerable persons or particularly sensitive data is anonymized where possible. BOM minutes are only distributed in paper copy and taken back following the completion of a meeting. Where emailed, the minutes will be password protected and sent to a school email address. Minutes are kept secure at all times and that the information is shredded as soon as could be reasonably expected. Relevant board members & employees briefed on the Data Protection Policy.
D076 **School Closure / Amalgamation Records**	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. Senior Management. Trustee.	N/a	On school closure, records should be transferred as per Records Retention Policy in the event of school closure / amalgamation. A de-commissioning exercise should take place with respect to archiving and recording data.	Do Not Destroy	**Technical:** Computers on which records are stored are password protected and are accessible only to designated staff. **Organisational:** Former student and staff files – to be returned to trustees. Appropriate measures established for former students and staff accessing these records.

35. Other School Based Reports / Minutes

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D077 **Principal's report including staff absences**	Confidential	**Electronic:** Principal's Office	Fulfil good governance and running of the school in the Public Interest.	Public Interest. Defence of Legal Claim.	Student Personal Data. Staff Personal Data.	Department of Education & Skills. Principal. Deputy Principal.	N/a	Indefinitely. Pending Review by the BoM.	Do Not Destroy.	**Technical:** Computers on which records are stored are password protected and are accessible only to designated staff. Principal's Office is locked when not in use. **Organisational:** Relevant staff briefed on the Data Protection Policy. Administrative log and does not relate to any one employee in particular: the monthly reports are not structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Not a "relevant filing system".

36. 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
D078 **Audited Accounts**	Confidential	**Paper:** Finance Office in locked and secure filing cabinets.	School Financial Accounts & Reporting	Public Interest. Legal Obligation.	Board of Management Signatories.	Trustee. FSSU. Board of Management. Principal. Revenue Commissioner.	N/a	Indefinitely. Pending Review by the BoM.	Do Not Destroy.	**Technical:** Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system. **Organisational:** Access to Financial Records is limited to authorised personnel i.e. Principal / Deputy Principal, Administrators.
D079 **Payroll and Taxation**	Confidential	**Paper:** Accounts Office in locked and secure filing cabinets. **Electronic:** Payroll Software	Process Payroll & Taxation.	Public Interest. Legal Obligation. Contractual Obligation.	Staff Personal Data incl. Name, PPSN, Address, Tax Credits.	Principal. Deputy Principal. Revenue Commissioner.	N/a	Indefinitely. Pending Review by the BoM.	Do Not Destroy.	**Technical:** Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system. **Organisational:** Access to Financial Records is limited to authorised personnel i.e. Principal & Administrators.
D080 **Invoices / Back Up Records / Receipts**	Confidential	**Paper:** Accounts Office in locked and secure filing cabinets. **Electronic:** Payroll Software	School Financial Accounts & Reporting	Public Interest. Legal Obligation. Contractual Obligation.	Vendor Information.	Principal. Deputy Principal. Revenue Commissioner.	N/a	7 years.	Confidential Shredding.	**Technical:** Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system. **Organisational:** Access to Financial Records is limited to authorised personnel i.e. Principal / Deputy Principal, Administrators.

37. 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
D081 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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Indefinitely.	Do Not Destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D082 Calculation of Service	Confidential	**Paper:** Principal's Office in locked and secure filing cabinets.	Pension Admins.	Public Interest. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teaching Council Number. Email. Career History.	Administrators. Principal. Deputy Principal.	N/a	Indefinitely.	Do Not Destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D083 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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Indefinitely.	Do Not Destroy.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D084 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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	18 months.	Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D085 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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	Retain original on personnel file and copy of master & appeal file. Retain for duration of employment + 7 years. Copy on master and appeal file.	Confidential Shredding.	**Technical:** Only the minimum data is collected from the data subject to fulfil our processing needs. Computers are password protected and are only accessible by designated staff. **Organisational:** Office is locked when not in use. Staff briefed on the Data Protection Policy.
D086 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. Teaching Council Number. Email. Career History.	Principal. Deputy Principal.	N/a	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.

38. Data Protection Communications – Data Protection Policy

- This document will be made known to all employees and staff as the primary source of Data Privacy Policy at Catholic University School.
- Employees and contractors will be formally notified of Catholic University School's position with respect to this policy via a staff briefing.

39. Data Protection Communications – Privacy Notices

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

- Identification of Catholic University School as the controller of personal data.
- A description of the personal data 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 Catholic University School.
- Summary technical details regarding information processing (including cookie use).

The Data Privacy Notice will be formatted appropriately for the medium in which it is published. The Data Privacy Notice is considered an advisory notice regarding Catholic University School policy and is not intended to constitute a contract with any person.

40. Data Protection Communications – Website Privacy Notice

Catholic University 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 Notice. The Privacy Notice will include at a minimum:

- Identification of Catholic University School as the data controller.
- A description of the personal data 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.
- Summary technical details regarding information processing (including cookie use).

41. Communication Plan for Privacy Notices

- Catholic University 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.
- Catholic University 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. parent(s) / guardian(s) of students) need to be informed more proactively regarding our use of their personal data, we will accomplish this by direct email to those users. This will be carried out in advance of the change going live. Where a change of use requires a response, the lack of a response will not be treated as acceptance.
- From time to time, it will be necessary to revise the Data Protection Policy as well as associated Privacy Notice in response to changes in regulations or evolution of expectations for compliance.
- The Privacy Notice itself contains an advisory to users to check regularly for changes.

42. Third Parties – Data Processors

Catholic University 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.

Catholic University 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 Catholic University 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.

43. Third Parties – Transfers of Personal Data to non-EEA jurisdictions

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

Catholic University School has identified the following Processors and the adequacy arrangements in place to ensure that these transfers are lawful under GDPR.

44. 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, Catholic University School will give immediate consideration to informing those affected. Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures.

In appropriate cases, Catholic University 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 and Skills 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, Catholic University 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 of a laptop hard drive) were of a high standard.

All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to Catholic University 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 becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects, and it does not include sensitive personal data or personal data of a financial / sensitive personal nature. If there is any doubt related to the adequacy of technological risk-mitigation measures, then Catholic University School will report the incident to the DPC.

Catholic University School will make report the breach to the DPC within 72 Hours of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial report will be online through their website and will include:

- 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 to those affected by the incident.
- A chronology of the events leading up to the breach.
- 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.

Even where there is no notification of the DPC, Catholic University 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.

45. Data Security Breach – Action Plan

Identification and Initial Assessment of the Incident

- Consider partial or complete systems lockdown.
- 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.

Containment and Recovery

- Establish who within the school needs to be made aware of the breach.
- Establish whether there is anything that can be done to recover the losses and limit the damage the breach could cause.
- 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).

Risk Assessment

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

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.

Evaluation and Response

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

46. Subject Access Requests

Data Subject Rights

Data Subjects, based upon a request made in writing to Catholic University School using the 'Subject Access Request Form' and upon successful verification of their identity, can obtain 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 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.

Student making a Subject Access Request

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

Parent(s) / Guardian making a Subject Access Request

- Where a parent(s) / guardian(s) makes an access request on behalf of his/her child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the parent(s) / guardian(s) 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(s) / guardian(s) subject to the provisions above.

Third Parties making a Subject Access Request

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

Logging 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 Subject Access Request Register.

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 the school to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.
- If the school cannot respond fully to the request within 30 days, the school shall 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 responses will be provided.
    - The name and contact information of Catholic University School individual who the Data Subject should contact for follow up.

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 a 3rd party. In such cases, information must be redacted as may be necessary or appropriate to protect that person's rights.

Right to Erasure

- The school shall erase the personal data of a data subject who requests the erasure of personal data concerning him or her without undue delay or will ensure the erasing of personal data without undue delay where one of the following grounds apply.
  - The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
  - The data subject withdraws consent on which the processing is based according to point (a) of article 6(1) 'Lawfulness of processing' or point (a) of article 9(2), 'Processing of special categories of personal data' the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. And where there is no other legal ground for the processing.
  - The data subject objects to the processing pursuant to article 21(1) 'right to object' and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) 'direct marketing':
  - The personal data has been unlawfully processed.
  - The personal data has to be erased for a legal obligation in Union or Member State law to which the controller is subject.
- A record of erasing the data subject's personal data shall be recorded and noted in the Board of Management Meeting Minutes.

47. Archiving Personal Data

Appraisal of Records
An appraisal process that limits the permanent preservation of records containing personal data to what is really necessary has been adopted. Personal Data containing significant historical value will be prioritised i.e. Photographs, Registers of Attendance / Enrolment, Academic Achievement in Second & Third Level Education, Sporting Achievements and photographs and video recordings of school and extracurricular activities and events may be selected for permanent preservation.

Data Minimisation:
Catholic University School will adhere to the principle of personal data minimisation i.e. only minimal data that is adequate, relevant and limited to what is necessary in relation to the purposes of permanent preservation.

Security:
Appropriate technical and organisational measures will be adopted including but not limited to alarming the archive room and restricting access to a small number of keyholders.

Data Subject Rights
Catholic University School will at all times observe Data Subject's Rights under GDPR.

Archiving Process
Catholic University School will archive personal data where this data has significant historical value. The school will not hold data for 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 significant historical value.
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 Schedule).
3. 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 preserved permanently for a specific lawful purpose (see Data Processing Map & Retention Schedule).
4. This step will involve:
    a. Consulting the Retention period as outlined in the Data Map & Retention Schedule.
    b. Identifying the records for disposal / archiving.
    c. Obtain permission from the Principal / BoM / Trustee to dispose / archive of the records.
    d. Document the disposal / archiving of records.
5. 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. Pending Review by the BoM.
6. Consultation should also take place with the Principal for advice on record retention periods for certain records as needed.
7. Archived boxes will be held securely in the school's dedicated archive with restricted access.

48. Disposal of Personal Data

Data Subject Rights

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

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

49. Governance

Supervisory Authority

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

Monitoring Compliance

Catholic University 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 Catholic University 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 Notices & Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.

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

Breaches of the Data Protection Policy

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 Code of Behaviour.

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.

50. Data Protection Policy Acknowledgement

Print Name	Signed	Date