Christian Brothers College

Data Protection Policy

Revision	Description	Approved By
Annual review	Data Protection Policy	Consultation Process: • Teaching Staff • Student Council • Parents Council • Preparatory School Ratified by the Board of Management:

Data Protection Policy

Purpose and Scope

1. The purpose of this Data Protection Policy is to support the College in meeting its responsibilities with regard to the processing of personal data. These responsibilities arise as statutory obligations under the relevant data protection legislation. They also stem from our desire to process all personal data in an ethical manner which respects and protects the fundamental rights and freedoms of natural persons.
2. This policy aims to help transparency by identifying how the College expects personal data to be processed. It helps to clarify what data is collected, why it is collected, for how long it will be stored and with whom it will be shared.
3. The Irish Data Protection Act (2018) and the European General Data Protection Regulation (GDPR) (2016) are the primary legislative sources. As such they impose statutory responsibilities on the College as well as providing several fundamental rights (for students, parents/guardians and staff and others) in relation to personal data.
4. The College recognises the seriousness of its data processing obligations and has implemented a set of practices to safeguard personal data. Relevant policies and procedures apply to all school staff, the Boards of Management, trustees, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school).
5. Any amendments to this Data Protection Policy will be communicated through the school website and other appropriate channels, including direct communication with data subjects where this is appropriate. The College will endeavour to notify a data subject if at any time we propose to use personal data in a manner that is significantly different to that stated in this Policy, or, if otherwise communicated at the time that it was collected.
6. The College is a data controller of personal data relating to its past, present and future staff, students, parents/guardians and other members of the school community. Formally, the statutory responsibility of Controller is assigned to the Board of Management. The Principal is assigned the role of co-ordinating the implementation of this Policy and for ensuring that all staff who handle or have access to personal data are familiar with their responsibilities.

Name	Responsibility
Board of Management	Data Controller
Principal	Implementation of Policy
All staff	Adherence to the Data Processing Principles
Entire College Community	Awareness and respect for all personal data

Processing Principles

1. Processing is the term used to describe any task that is carried out with personal data e.g. collection, recording, structuring, alteration, retrieval, consultation, erasure as well as disclosure by transmission, dissemination or otherwise making available. Processing can include any activity that might relate to personal data under the control of the College, including the storage

of personal data, regardless of whether the records are processed by automated or manual means.

2. There are several fundamental principles, set out in the data protection legislation, that legally govern the College's treatment of personal data. As an integral part of its day-to-day operations, the College will ensure that all data processing is carried out in accordance with these processing principles.
3. These principles, set out under GDPR, establish a statutory requirement that personal data must be:
    a. processed lawfully, fairly and in a transparent manner.
    b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
    c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
    d. accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
    e. kept for no longer than is necessary for the purposes for which the personal data are processed.
    f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
4. GDPR also establishes accountability as a core data processing principle. This places a statutory responsibility on the College, as Data Controller, to be able to demonstrate compliance with the other principles i.e. the six data processing principles set out in the previous paragraph (3 above).

Lawful Basis for Processing Personal Data

1. Whenever the College is processing personal data, all of the principles listed in the previous sections, will be obeyed. In addition, at least one of the following bases (GDPR Article 6) must apply if the processing is to be lawful:
    a. compliance with a legal obligation
    b. necessity in the public interest
    c. legitimate interests of the controller
    d. contract
    e. consent
    f. vital interests of the data subject.
2. When processing special category personal data, the College will ensure that it has additionally identified an appropriate lawful basis under GDPR Article 9. Special categories of personal data are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing Activities Undertaken by the College

1. Record of Processing Activities
   This policy sets out the purposes for which the College collects and uses personal data for each of the various categories of data held (student, staff, parent, etc).
2. Student Records
   The purposes for processing student personal data include the following:
   a. to provide information prior to application/enrolment.
   b. to determine whether an applicant satisfies the College's admission criteria.
   c. to comprehend the educational, social, physical and emotional needs of the student.
   d. to deliver an education appropriate to the needs of the student.
   e. to ensure that any student seeking an exemption from Irish meets the criteria.
   f. to ensure that students benefit from relevant additional educational or financial supports.
   g. to contact parents/guardians in case of emergency or in the case of school closure.
   h. to monitor progress and to provide a sound basis for advising students and parents/guardians.
   i. to inform parents/guardians of their child's educational progress etc.
   j. to communicate information about, and record participation in, school events, etc.
   k. to compile yearbooks, establish a school website, and to keep a record of the history of the school.
   l. to comply with legislative or administrative requirements.
   m. to furnish documentation/ information about the student to the Department of Education and Skills (DES), the State Exams Commission (SEC), the National Council for Special Education (NCSE), TUSLA – Child and Family Agency, and others in compliance with law and directions issued by government departments.
3. Parent/Guardian Records
   The College does not keep personal files for parents or guardians. However, information about, or correspondence with, parents may be held in the files for each student. This information shall be treated in the same way as any other information in the student file.
4. Staff Records
   As well as records for existing members of staff (and former members of staff), records may also relate to applicants applying for positions within the College, trainee teachers and teachers under probation. The purposes for which staff personal data is processed include the following:
   a. the management and administration of school business (now and in the future).
   b. to facilitate the payment of staff and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant).
   c. to facilitate pension payments in the future.
   d. human resources management.
   e. recording promotions made (documentation relating to promotions applied for) and changes in responsibilities, etc.
   f. to enable the College to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare at Work Act, 2005).
   g. to enable the school to comply with requirements set down by the DES, the Revenue Commissioners, the NCSE, TUSLA, the Health Service Executive (HSE), and any other governmental, statutory and/or regulatory departments and/or agencies.

h. and for compliance with legislation relevant to the College.

5. Board of Management Records
   Board of Management records are kept in accordance with the Education Act 1998 and other applicable legislation. Minutes of Board of Management meetings record attendance, items discussed and decisions taken. Board of Management business is considered confidential to the members of the Board.
6. Financial Records
   This information is required for routine management and administration of the College's financial affairs, including the payment of fees, invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.
7. CCTV Records
   The College processes personal data in the form of recorded CCTV images. We use CCTV for the following purposes:
   a. to secure and protect the College's premises and assets.
   b. to deter crime and anti-social behaviour.
   c. to assist in the investigation, detection, and prosecution of offences.
   d. to monitor areas in which cash and/or goods are handled.
   e. to deter bullying and/or harassment.
   f. to maintain good order and ensure the College's Code of Behaviour is respected.
   g. to provide a safe environment for all staff and students.
   h. for the taking and defence of litigation.
   i. for verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and where the recordings may be capable of resolving that dispute.

   Further information is available in the College's CCTV Policy.

Recipients

1. Recipients
   These are defined as organisations and individuals to whom the College transfers or discloses personal data. Recipients may be data controllers, joint controllers or processors. A list of the categories of recipients used by the College is provided in the appendices (Appendix 3). This list may be subject to change from time to time.
2. Data Sharing Guidelines
   a. From time to time the College may disclose personal data to third parties or allow third parties to access specific Personal data under its control. An example could arise should an Garda Síochána submit a valid request under Section 41(b) of the Irish Data Protection Act which allows for processing necessary and proportionate for the purposes of preventing, detecting, investigating, or prosecuting criminal offences.
   b. In all circumstances where personal data is shared with others, the College will ensure that there is an appropriate lawful basis in place (GDPR Articles 6, 9 as appropriate). The College will not share information with anyone without consent unless another lawful basis allows us to do so.
   c. Most data transfer to other bodies arises because of the College's legal obligations, and the majority of the data recipients are Controllers in their own right, for example, the DES. As such, their actions will be governed by national and European data protection legislation as well their own organisational policies.

d. Some of the College's operations require support from specialist service providers. For example, the College may use remote IT back-up and restore services to maintain data security and integrity. In cases such as these, the College will ensure that the appropriate security guarantees have been provided and that there is a signed processing agreement in place.

Personal Data Breaches

1. Definition of a Personal Data Breach
   A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
2. Consequences of a Data Breach
   a. A breach can have a significant adverse effect on individuals, which can result in physical, material or non-material damage. This can include discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality, etc. Children because of their age may be particularly impacted.
   b. In addition to any detrimental impact on individual data subjects, a data breach can also cause serious damage to the College. This can include reputational damage as well as exposing the school to other serious consequences including civil litigation.
   c. It should be noted the consequences of a data breach could include disciplinary action, criminal prosecution and financial penalties or damages for the school and participating individuals.
3. Responding to a Data Breach
   a. The College will always act to prioritise and protect the rights of those individuals whose personal data is affected.
   b. As soon as the College becomes aware that an incident has occurred, measures will be taken to assess and address the breach appropriately, including actions to mitigate any possible adverse effects.
   c. Where the College believes that there is a risk to the affected individuals, it will (within 72 hours of becoming aware of the incident) submit a report to the Data Protection Commission.
   d. Where a breach is likely to result in a high risk to the affected individuals, the College will inform those individuals without undue delay.

Data Subject Rights

1. Rights
   Personal Data will be processed by the College in a manner that is respectful of the rights of data subjects. Under GDPR these include:
   a. the right to information.
   b. the right of access.
   c. the right to rectification.
   d. the right to erasure (right to be forgotten).
   e. the right to restrict processing.
   f. the right to data portability.
   g. the right to object.

h. the right not to be subject to automated decision making.
i. the right to withdraw consent.
j. the right to complain.

2. Right to be Informed
   Data subjects are entitled to information about how their personal data will be processed. The College address this right primarily through the publication of this Data Protection Policy. We also publish additional privacy notices/statements which we provide at specific data collection times, for example, our Website Data Privacy Statement is available to all users of our website. Any person who requires further clarification or information that is not explicit in our Policy or Privacy Statements, is requested to forward their query to the College.
3. Right of Access
   Data subjects are entitled to see any information the College holds about them. The College will, on receipt of a request from a data subject, confirm whether their personal data is being processed. In addition, a data subject can request a copy of their personal data. The College in responding to a right of access will ensure that it does not adversely affect the rights of others.
4. Right to rectification
   If a data subject believes that the College holds inaccurate information about them, they can request that the information be corrected. The personal record may be supplemented with additional material where it is adjudged to be incomplete.
5. Right to be forgotten
   Data subjects can ask the College to erase their personal data. The College will act on such a request providing that there is no compelling purpose or legal basis necessitating retention of the personal data concerned.
6. Right to restrict processing
   Data subjects have the right to seek a restriction on the processing of their data. This restriction gives an individual an alternative to seeking erasure of their data. It may also be applicable in other circumstances such as where, for example, the accuracy of data is being contested.
7. Right to data portability
   This right facilitates the transfer of personal data directly from one controller to another. It can only be invoked in specific circumstances, for example, when processing is automated and based on consent or contract.
8. Right to object
   Data subjects have the right to object when processing is based on the College's legitimate interests or relates to a task carried out in the public interest (e.g. the processing of CCTV data may rely on the College's legitimate interest in maintaining a safe and secure school building). The College must demonstrate compelling legitimate grounds if such processing is to continue.
9. Right not to be subject to automated decision making
   This right applies in specific circumstances (as set out in GDPR Article 22).
10. Right to withdraw consent
    In cases where the College is relying on consent to process a person's data, the person has the right to withdraw this at any time, and if they exercise this right, the College will stop the relevant processing.
11. Limitations on Rights
    While the College will always facilitate the exercise of a data subject's rights, it is recognised that the College may also need to consider other obligations.
12. Right to Complain

a. If a data subject is concerned about how their personal data is being processed, these concerns must be addressed in the first instance to the Principal who is responsible for operational oversight of this policy.
b. A matter that is still unresolved may then be referred to the College's Data Controller (i.e., the Board of Management) by writing to the Chairperson of the Board of Management.
c. If a data subject is still dissatisfied with how the College has addressed a complaint or concern that they have raised, they have the right to bring the matter to the attention of the Irish Data Protection Commission. Contact details are available at www.dataprotection.ie

Ratified by the Board of Management at its meeting of 18th April 2024

Laurence Nash 18/4/24
Chairperson

David Lordan 18/4/24
Principal

Appendix 1 Glossary

Child – a person under the age of 18 years. Children are deemed as vulnerable under GDPR and merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Controller or Data Controller – an entity or person who, alone or jointly with others, determines the purposes and means of the processing of personal data. In this policy, the data controller is the College.

Consent – any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

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

Data Protection Legislation – this includes (i) the General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and (ii) the Irish Data Protection Act (2018). GDPR is set out in 99 separate Articles, each of which provides a statement of the actual law. The regulation also includes 171 Recitals to provide explanatory commentary.

Data Subject – a living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

Data concerning health – personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. This is an example of special category data (as is data concerning special education needs).

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

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor or Data Processor – a person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract (but does not include an employee of a controller who processes such data in the course of his or her employment).

Profiling – any form of automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

(Relevant) Filing System – any set of information that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

Special categories of data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Appendix 2 Personal Data and Data Related Processing Purposes

Purposes for Processing	Description of Personal Data
1. Contact and Identification Information This information is needed to identify, contact and enrol students.	
Purposes may include: • To add names to a contact list prior to formal application. • To provide appropriate information to prospective pupils. • To make contact in case of school closure (e.g. adverse weather conditions). • To send SMS text messages and emails about meetings, etc.	Information required to confirm student/parent identity and contact through communications. • Student name. • Gender. • Date of birth. • Family details (parents/guardian names, addresses, contact details to include phone numbers, email addresses, etc.
2. Application Information This information used to determine whether an applicant meets the eligibility requirements as set out in the College Admissions Policy.	
In addition to data outlined at (1) above, we collect personal data via application forms and student transfer forms. Where the student is offered a place, completed application forms are placed on the student's file. Where the student is not offered a place, the data will be used for the purposes of responding to any Section 29 appeals process. Applicants may opt to provide data on religion at this stage where this forms part of the school's admissions criteria. Any information not required to operate the admissions procedure, is identified as optional.	Information as required to ascertain eligibility under the College's Admissions Policy: • Name and address of current school. • Class in current school. • Details of siblings, etc. • Religion (based on consent).
3. Enrolment Information Once the College has accepted the student's application, and has offered the student a place, other information is collected in addition to the data outlined at (1) and (2) above. This personal data is used for administrative and management tasks e.g. school communications, timetabling, scheduling parent teacher meetings, school events, arrangements for academic registration, class details, start dates, book lists, subject-selection, school trips etc.	
Contact and identification information. We use this information: • To make contact in case of school closure (e.g. adverse weather conditions), or an emergency (ill-health or injury). • To communicate issues relating to progress, welfare or conduct in school, non-attendance or late attendance, etc. • To send SMS text messages and emails about important events, e.g. start dates, course details, meetings, school events, etc.	• Student name and date of birth (requires birth certificate verification by school). • PPSN. • Address including Eircode. • Extended family details (parent/guardian names, contact details, postal and email address, phone numbers, addresses, details of any court orders or other arrangements governing access to, or custody of, child). • Details of next of kin (for contact in case of emergency).
Academic Record. We use this information to deliver education appropriate to the needs of the student, to	• Reports, references, assessments and other records from any previous school(s) attended by the student.

assess the student's educational progress. standardised test results used for the purposes of assessing literacy/numeracy progress, for reasonable accommodation in state examinations, for assisting in referrals to the National Educational Psychological Service (NEPS), and for career guidance etc.	• Education passport (6th class report provided by primary school after post-primary school confirms enrolment. protocols set out in des circulars 42/2015 and 34/2016). • Standardised testing results.
Language Spoken. Without this information the College will not know how to meet the student's needs and to deliver appropriate education. This ensures the student has access to language support (where necessary). Irish Exemption. Information regarding application for Irish exemption if eligible (e.g. received primary school up to 11 years of age outside Ireland, evidence of disability, student from abroad etc).	• Information about language spoken (for language support). • Details of whether the student received English as an additional language (EAL) support. • Details regarding whether the student is exempt from studying Irish. • Details to ascertain if the student is eligible for exemption from study of Irish.
Medical information for health purposes. This information is essential to meet our duty of care to the student. We use this information to: (i) ensure we know who to contact in case of emergency. (ii) ensure that we have relevant information to safeguard/prevent damage to student health. (iii) meet medical/care needs when students are in school. (iv) facilitate appropriate advanced planning with parents/guardians (e.g. notification to relevant personnel within the school, storage of medications, staff training where necessary, etc).	• Emergency contact details (name, telephone, details of relationship to the student, etc). • Details of the student's GP (to be contacted in case of emergency). • Details of any relevant medical information (e.g. medical condition, allergies, treatment/care plan etc) to facilitate appropriate advanced planning with parents/guardians. This may include use of student's photograph for display in the staff room as part of the emergency action plan.
Additional Educational Needs (AEN) and medical information for educational purposes. We cannot meet our duty of care to the student and our obligations under the Education for Persons with Special Educational Needs Act (EPSEN), 2004 without this information. We use this information to: (i) make application to the des for allocation of resources to support student. (ii) ensure school has relevant information to deliver education appropriate to student's needs. (iii) apply for appropriate accommodation(s) and/or therapeutic supports where available.	• Details of any AEN/medical needs that need to be accommodated, e.g. medical assessment, hearing/vision issues, psychological assessment/report. • Details of whether the student has been in receipt of learning support. • Details of whether the student been granted learning support hours and/or additional needs assistance hours by the NCSE.
Information sought by the DES. The College is under a legal obligation to return specific enrolment information concerning	Personal data is transferred to the DES via the post-primary online database as set out in the privacy notice for p-pod provided by DES.

each student to DES (SI 317/2015). This data is used to calculate teacher and resource allocation, capitation, grant payments for schools, for statistical analysis and reporting in the areas of social inclusion and integration of students in the education system, and for planning purposes. Other (optional) information is sought for purposes relating to planning, social inclusion and integration of students in the education system.	Required information includes, e.g. birth name of student and mother (to verify student identity). The DES seeks some additional information on an optional basis (i.e. based on parental consent), for example, ethnic/cultural background.
Use of photographs for yearbooks, social media, website etc. Photographs, and recorded images of students may be taken at school events and to celebrate school achievements, to compile yearbooks, to display on the College website, to record College events, and to keep a record of the history of the College.	• Consent to use (for these purposes) images or recordings in printed or digital format. • Separate consents will be sought for different publication forums, NB this excludes CCTV recordings – see the College's CCTV Policy.
Religion is only sought where the school facilitates religious instruction/faith formation at the request of parent(s)/ guardian(s).	Religious denomination (based on consent).
Consents to direct marketing. Anybody who wishes to receive direct marketing can give consent for the College to contact you by SMS text and/or email. The right to opt-out only relates to the College making contact for direct marketing purposes.	Note: the College will still contact you on your mobile in case of an emergency relating to your child and/or to communicate messages about school events (e.g. school closure, parent-teacher meetings etc).
4. Personal data gathered during student's time in school. We cannot meet our statutory obligation to deliver appropriate education to students and/or we cannot satisfy our duty of care to each student without processing this information.	
Academic Progress. The College processes this personal data in order to deliver education to students, and to evaluate students' academic progress, to register the student for state examinations (Junior Cycle, Leaving Certificate), to submit the students' work to the recognised accrediting body, etc.	• Academic progress and results. • State exam results. • Results of in-school tests/exams (end of term, end of year exams, assessment results). • Continuous assessment and end of term/year reports.
Attendance. The College is required to collect and monitor attendance data and to notify the Education Welfare Officer (TUSLA) in certain circumstances, such as: (i) where the student is suspended for six days or more. (ii) where the student is absent for an aggregate period of 20 school days during the course of the year. (iii) where the Principal is of the opinion that the student is not attending school regularly. The College will notify parent/guardian in the	Statutory processing pursuant to the Education (welfare) Act 2000. • Attendance records including registers and roll books etc. • Records of referrals to TUSLA. School register and roll books are documents of enduring historical value and are retained in the College's archives for archival purposes in the public interest.

event of non-attendance or absences.	
School tours/trips. Information required to make appropriate travel arrangements, to implement insurance cover, to arrange appropriate supervision ratios, to ensure medical/health issues are properly accommodated, to engage in responsible planning, and to ensure necessary paperwork for INIS (Irish border control/Irish naturalisation and immigration service requirements where children are travelling with someone other than their parent or guardian). Further information is available in the College's School Tours Policy.	Information to ensure trip is properly organised and supervised, including: • Permission slips (signed by parents/guardians). • Itinerary reports. • Letter from parent(s)/guardian(s) giving consent to travel. • Copy of birth/adoption certificate or guardianship papers. • Copy of marriage/divorce certificate (where parent has different surname to child). • Copy of the parent/guardian's passport or state identity document.
Garda vetting outcomes. Certain work experience roles may require that a student be Garda vetted (statutory vetting process).	Information as set down in National Vetting Bureau (Children and Vulnerable Persons) Act 2012. • Garda vetting form.
CCTV images. The school processes this data for the purposes outlined in our CCTV policy, a copy of which is available on the school's website e.g. we use CCTV for security purposes; to protect premises and assets; to deter crime and anti-social behaviour; to assist in the investigation, detection, and prosecution of offences; to monitor areas in which cash and/or goods are handled; to deter bullying and/or harassment; to maintain good order and ensure the school's code of behaviour is respected; to provide a safe environment for all staff and students; for verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and the recordings may be capable of resolving that dispute; for the taking and defence of litigation.	CCTV is in operation at the perimeter, exterior and certain internal common areas within the College both during the daytime and during the night hours each day. CCTV is used at external points on the premises (e.g. at front gates, in the carpark etc) and at certain internal points (e.g. reception area, corridors, etc). in areas where CCTY is in operation, appropriate notices will be displayed.
Additional educational needs data, educational support records, medical data etc. Without this information, the College will not know what resources need to be put in place to meet the student's needs and to deliver appropriate education in-keeping with its statutory obligations. This is to assess student needs, determine whether resources can be obtained and/or made available to support those needs, and to develop individual education plans. Under Section 14 of the EPSEN Act, 2004, the College is required to furnish to the NCSE (the statutory agency established under the EPSEN Act 2004) such information as the Council may from time-to-time reasonably	The College collects information relating to any additional educational needs, psychological assessments/reports, information about resource teaching hours and/or additional needs assistance hours, etc. Schools are also required to share this personal data with SENOs employed by the NCSE. • Psychological assessments. • Additional educational needs' files, reviews, correspondence. • Individual education plans. • Learning support file. • Notes relating to inter-agency meetings. • Medical information (including details of any medical condition and/or

request.	medication/treatment required). • Psychological, psychiatric and/or medical assessments.
Child protection, child welfare records. The College is required to follow the DES Child Protection Procedures for Primary and Post-Primary Schools (revised 2023) and to take appropriate action to safeguard the welfare of students in its care. Staff have a legal responsibility to report actual or suspected child abuse or neglect to TUSLA and to an Garda Síochána. Mandatory reporting obligations arise under Children First 2015, the Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012. All relevant data is stored in a dedicated fireproof safe accessible by the DLP and Deputy DLP only in line with child protection requirements.	Mandatory reporting obligations require data sharing with TUSLA, an Garda Síochána and any other appropriate law enforcement or child protection authorities. DES Inspectorate may seek access to the school's child protection records for audit purposes. • Child protection records. • Child safeguarding records. • Other records relating to child welfare. • Meitheal meetings convened by TUSLA.
Counselling and Pastoral Care Records. This information is required to provide access to counselling services and/or psychological services and to provide supports to students, resolve behavioural, motivational, emotional and cognitive difficulties through assessment and therapeutic intervention, to engage in preventative work, etc. Personal data (and special category personal data) will be shared with third parties such as TUSLA, NEPS, the Child and Adolescent Mental Health Service (CAMHS), An Garda Síochána and medical practitioners treating the student, for the purpose of the College complying with its legal obligations and/or in the student's vital/best interests.	• Guidance counselling notes. • Psychological service notes. • Referrals to/records relating to therapeutic services and other interventions. • Minutes, notes and other records concerning student support team meetings.
Internal school processes. This information (e.g. anti-bullying processes and Code of Behaviour processes) is required to meet the College's duty of care to all its students and staff, to comply with relevant circulars issued by the DES, and to run the school safely and effectively. Data collected in these processes may be transferred to the school's insurer and/or legal advisors or management body as appropriate where required for disputes resolution, fact verification, and for litigation purposes.	• Records of parental complaints. • Records of other complaints (student to student complaints etc). • Records relating bullying investigations. • Records relating to Code of Behaviour processes (expulsion, suspension etc.) including appeals data and Section 29 appeals material.
Accident and injury reports. This information is processed to operate a safe environment for students and staff, to identify	• Accident reports. • Incident report forms. • Notifications to insurance company.

and mitigate any potential risks, and to report incidents/accidents. This data may be transferred to the school's insurance company and/or indemnifying body and/or legal advisors as appropriate. Data will be shared with an Garda Síochána, TUSLA and the Health and Safety Authority (HSA) where appropriate.	• Exchanges with legal advisors. • Notifications to the HSA.
Financial information, fees, etc. Without this information, the College cannot process applications, make grant payments, or receive payment of monies (e.g. course fees, school trips etc). After completion of the payments, the documentation is retained for audit and verification purposes. The College's financial data are audited by external auditors.	• Information relating to payments from student's parents/guardians (including fee support and fee waiver documentation). • Scholarship/grant applications (including Gaeltacht, book rental scheme etc).
5. Charity Tax Back Forms This information is required so that the College may avail of the scheme of tax relief for donations of money received.	
To claim the relief, the donor must complete a certificate and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. This information is retained by the school in the case of audit by the revenue commissioners.	• CHY3/CHY4 tax back forms. • Donor name, address & telephone number. • PPS number. • Tax rate. • Signature. • Gross amount of donation.
6. Parent Nominees on Boards of Management This information is required to enable the Board of Management to fulfil its statutory obligations.	
Processing undertaken in accordance with the Education Act 1998 and other applicable legislation, including decisions taken for accountability and good corporate governance.	• Name, address and contact details of parent nominee. • Records in relation to appointment to the Board. • Minutes of Board of Management meetings and correspondence to the Board.

Appendix 3 Categories of Recipients

Department of Education and Skills (DES)

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

State Examinations Commission (SEC).

Data on entrants for the state examinations is provided via the October Returns to SEC to assist its planning of the state examinations.

Student support and welfare.

Student data may be shared with a number of public state bodies including NEPS (psychologists to support schools and students), NCSE (to support schools and students with additional education needs); TUSLA (the College is required to share student attendance with TUSLA). Data to support student access to further and higher education may also be shared for processing as part of Student Universal Support Ireland (SUSI), Higher Education Access Route (HEAR) and Disability Access Education Route (DARE).

Legal requirements

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

Insurance

Insurance data may be shared with the College's insurers where this is appropriate and proportionate. The College may also be obliged to share personal data with the HSA, for example, where this is required as part of an accident investigation.

Professional Advisors

Some data may be shared with legal advisors (solicitors, etc.), financial advisors (pension administrators, accountants, etc.) and others such as school management advisors; this processing will only take place where it is considered appropriate, necessary and lawful.

Other Schools and Universities/Colleges/Institutes

Where the student transfers to another educational body, or goes on an exchange programme or similar, the College may be asked to supply certain information about the student, such as academic record, references, etc.

Work Placement

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

Voluntary Bodies

Some personal data may be shared as appropriate with bodies such as the College's Parents Council. This data sharing will only take place where consent has been provided.

Other not-for-profit organisations

Limited data may be shared with recognised bodies who act to promote student engagement with co-curricular and other activities, competitions, recognition of achievements, etc. This would include bodies promoting participation in sports, arts, sciences, environmental and outdoor activities, etc. This data sharing will usually be based on consent.

Service Providers

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

- School Management Information Systems (VSWare).
- Productivity Applications (Google Workspace for Education).
- Online Storage & File Sharing (Google Drive).
- Video Sharing and Blogging Platforms (e.g. Youtube, Wordpress).
- Virtual Learning Environments (Google Classroom).
- IT Systems Support (local ICT Support Company)
- Fee management software (x)
- School communications (x)
- Security and CCTV Systems (x)
- Pension Consultants/Trustees (x)
- Accounting & Payroll software (x)
- Cashless Payment Systems (x)
- Canteen Management System (x)
- Learning software and Apps (x)

Transfers Abroad

In the event that personal data may be transferred outside the European Economic Area (EEA) the College will ensure that any such transfer, and any subsequent processing, is carried out in strict compliance with recognised safeguards or derogations (i.e., those approved by the Irish Data Protection Commission).

Appendix 4 Implementing the Data Processing Principles

1. Accountability
   a. Accountability means that compliance with the data protection legislation is recognised as an important Board of Management responsibility as well as one shared by each College employee and member of the wider College community.
   b. Demonstrating Compliance
      Accountability imposes a requirement on the controller to demonstrate compliance with the other data processing principles (see Section 2 earlier: Processing Principles). This means that the College retains evidence to demonstrate the actions it has taken to comply with GDPR.
   c. School Policies
      An important way for the College to demonstrate accountability is through the agreement and implementation of appropriate policies. In addition to publishing this Data Protection Policy, this may include developing other policies to address some or all of the following areas (i) CCTV (ii) Data Breaches (iii) Data Access Requests (iv) Record Storage and Retention (v) Data Processing Agreements.
   d. Record of Processing Activities
      As a data controller the College is required to prepare a record of any processing activities (ROPA) that it undertakes. This record will include the following information (GDPR Article 30):
         i. the purposes of the processing.
         ii. a description of the categories of data subjects and personal data.
         iii. the categories of recipients to whom the personal data will be disclosed.
         iv. any transfers to a third country or international organisation, including suitable safeguards.
         v. where possible, the envisaged time limits for erasure of the different categories of data.
         vi. where possible, a general description of the technical and organisational security measures.
   e. Risk Assessment
      The College as data controller is required to consider any risks that may arise as a consequence of its processing activities. This assessment will consider both the likelihood and the severity of these risks and their potential impact on data subjects.
   f. Data Protection Impact Assessment (DPIA)
      A DPIA is a type of risk assessment that is mandatory in specific circumstances (GDPR Article 35). The College will ensure that a DPIA is undertaken where this is appropriate, typically, where a new processing activity has the potential to have a high impact on individual privacy or rights. The installation of an extensive CCTV system in a school is an example of a processing activity that might trigger the need for a Data Protection Impact Assessment. The purpose of undertaking a DPIA is to ensure that any risks associated with the new processing activity are identified and mitigated in an appropriate manner.
   g. Security of Processing
      As a consequence of having assessed the risks associated with its processing activities, the College will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. For example, these measures might include training of

staff, establishment of password policies, protocols around device encryption, procedures governing access to special category data etc.

h. Data Protection by Design
The College aims to apply the highest standards in terms of its approach to data protection. For example, College staff will utilise a Privacy by Design approach when any activity that requires the processing of personal data is being planned or reviewed. This may mean implementing technical measures (e.g. security) and organisational measures (e.g. protocols and training).

i. Data Protection by Default
A Privacy by Default approach means that minimal processing of personal data is the College's default position. In practice this means that only essential data will be collected from data subjects, and that within the College, access to this data will be carefully controlled and only provided to employees where this is appropriate and necessary.

j. Data Processing Agreements.
The College will put written contracts in place with organisations that process data on its behalf (as required under GDPR Article 28).

k. Data Breach Records.
The College will retain records that document its handling of any personal data breaches. These records will clearly set out the facts relating to any personal data breach, its effects and the remedial action taken.

l. Staff Awareness and Training.
All who are granted access to personal data that is under the control of the College have a duty to observe the data processing principles. The College will provide appropriate information, training and support so that staff may gain a clear understanding of these requirements.

2. Lawful Processing

As part of its decision to collect, use or share personal data, the College as Controller will identify which of the lawful bases is applicable to each processing operation. In the absence of a lawful basis the personal data cannot be processed.

a. Many of College 's data processing activities rely on legal obligations. These tasks are undertaken because the school must comply with Irish (or European) law. For example, there is a legislative basis underpinning the sharing of specific student data with the DES and other public bodies.

b. Another set of data processing activities are undertaken in the public interest i.e. so that the College can operate safely and effectively. For example, an educational profile of the student (literacy competence, language spoken at home, etc.) may help the College to target learning resources effectively for the benefit of the student.

c. In some situations, for example the use of CCTV, the College may rely on its legitimate interests to justify processing. In such cases the specific legitimate interests (e.g. health and safety, crime prevention, protection of the College property, etc.) will be identified and notified to the data subjects.

d. Contract will provide a lawful basis for some processing of data by the College. For example, the processing of some employee data may rely on this lawful basis.

e. There is also the possibility that processing can be justified in some circumstances to protect the vital interests of a data subject, or another person. For example, sharing some data subject data with emergency services might rely on this lawful basis.

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

3. Consent

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

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

4. Special Category Data

Some personal data is defined as Special Category Data and the processing of such data is more strictly controlled. In a school context this will occur whenever data that relates to Special Needs or Medical Needs is being processed. GDPR Article 9 identifies a limited number of conditions, one of which must be applicable if the processing of special category data is to be lawful. Some of these processing conditions, those most relevant in the school context, are noted here.

a. Processing is necessary for reasons of substantial public interest on the basis of European Union (EU) or Member State law. This condition could provide an appropriate basis for processing of data relating to employee and student health e.g. proportionate sharing of special category data to ensure the College is compliant with provisions in health, safety and welfare legislation.
b. Processing is necessary for the assessment of the working capacity of an employee; or for the provision of health or social care or treatment... based on EU or Member State law.
c. Processing is based on Explicit Consent. Where a school is processing biometric data for identification purposes (e.g. facial image recognition or the use of fingerprint systems) it is unlikely that this processing will be justifiable on any lawful basis other than consent. As a data subject should be able to withhold consent without suffering any detriment, the College will provide access to an alternative processing option which is not reliant on biometric data.

5. Transparency

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

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

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

7. Data Minimisation

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

a. The College will ensure, when data is being collected from data subjects, that this is limited to what is necessary for the completion of the duties. For example, where information is being collecting from students and parents/guardians, as part of the admissions process, this will be limited to whatever information is needed to operate the admissions process. This means that it is usually not appropriate for the College to seek information about AEN to decide whether a place should be offered.
b. Data minimisation also requires that the sharing of student data within the College should be carefully controlled. Members of staff may require varying levels of access to student data and reports. Access will be restricted to those who have a defined processing purpose.

Staff will not access personal data unless processing is essential to deliver on their role within the College.

c. College staff will necessarily create personal data in the course of their duties. However, employees will ensure that this processing is necessary and appropriate. For example, while it will often be necessary for College staff to communicate information to each other by email, consideration will be given, on a case by case basis, as to whether it is necessary for personal data to be included in these communications.
d. Data sharing with external recipients will be continuously reviewed to ensure it is limited to that which is absolute necessary. This may mean, for example, that when the College is seeking professional advice, no personal data will be included in communications unless the disclosure of this information is essential.

8. Storage Limitation

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

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

9. Integrity and Confidentiality

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

a. College employees are required to always act in a manner that helps to maintain the confidentiality of any data to which they have access. Guidance and training are important to help identify and reinforce appropriate protocols around data security.
b. The College is legally required to consider the risks to the data subject when any processing of personal data is taking place under its control. Any risk assessment will take particular account of the impact of incidents such as accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, the personal data.
c. As well considering the potential severity of any data incident, a risk assessment should also consider the likelihood of any incident occurring. In this way risks are evaluated on the basis of an objective assessment, by which it is established whether the data processing operations involve a risk or a high risk.

d. The follow-on from any risk assessment is for the College to implement appropriate technical and organisational measures that ensure a level of security appropriate to the risk. These measures will ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected (GDPR Recital 83).

e. As well as processing activities undertaken by staff, the College will also consider the risks associated with any processing that is being undertaken on behalf of the College by other individuals or organisations (Data Processors). Only processors who provide sufficient guarantees about the implementation of appropriate technical and organisational measures will be engaged.

f. The important contribution that organisational policies can make to better compliance with the accountability principle was previously highlighted. The following policies and protocols will each abide by the data protection requirements.

    i. Acceptable User Policy
    ii. Remote Working and Online Learning Policy
    iii. Passwords for College email, Google Classroom, Google Drive, computers, ipads.
    iv. Only College owned devices can be used for recording students in either picture, audio or video format.
    v. All audio and visual recordings and photos of students can only be shared via a College email account or on Google Drive.

Appendix 5 Managing Rights Requests

1. Responding to rights requests
    a. The College will log the date of receipt and subsequent steps taken in response to any valid request. This may include asking the data subject to complete an Access Request Form in order to facilitate efficient processing of the request. There is no charge for this process.
    b. The College is obliged to confirm the identity of anyone making a rights request and, where there is any doubt on the issue of identification, will request official proof of identity (e.g. photographic identification such as a passport or driver's licence).
    c. If requests are manifestly unfounded or excessive, in particular because of their repetitive character, the College may either:
        i. charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested.
        ii. refuse to act on the request.
    d. The College will need to confirm that sufficient information to locate the data requested has been supplied (particularly if CCTV footage/images are to be searched). Where appropriate the College may contact the data subject if further details are needed.
    e. In responding to rights requests (e.g. data access requests) the College will ensure that all relevant manual and automated systems (computers, etc.) are checked.
    f. The College will be conscious of the need to respond without undue delay and within the advised timeframes. A response will be made within one month of receipt of any request.
    g. The College will be conscious of the restrictions that apply to rights requests. Where unsure as to what information to disclose, the College reserves the right to seek legal advice.
    h. Where a request is not being fulfilled, the data subject will be informed as to the reasons and the mechanism for lodging a complaint, including contact details for the Data Protection Commission.
    i. Where action has been taken by the College with regard to rectification, erasure or restriction of processing, the College will ensure that relevant recipients (i.e. those to whom the personal data has been disclosed) are appropriately informed.
2. Format of information supplied in fulfilling a request
    a. The information will be provided in writing, or by other means, including where appropriate, by electronic means. When requested by a data subject the information access may be provided in alternative means e.g. orally.
    b. The College will endeavour to ensure that information is provided in an intelligible and easily accessible format.
    c. Where a request relates to video, the College may offer to provide the materials in the form of a series of still images. If other people's images cannot be obscured, then it may not prove possible to provide access to the personal data.

Reference Sites

Data Protection Act 2018 http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

General Data Protection Regulation (GDPR official text) 2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj

General Data Protection Regulation (GDPR unofficial web version) 2016 https://gdpr-info.eu/

GDPR for Schools website https://gdpr4schools.ie/

Data Protection for Schools http://dataprotectionschools.ie/en/

Irish Data Protection Commission https://www.dataprotection.ie/

Data Breach Report https://forms.dataprotection.ie/report-a-breach-of-personal-data

European Data Protection Board (EDPB) https://edpb.europa.eu/

EDPB Guidelines, Recommendations and Best Practices on GDPR https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

DES Data Protection Page https://www.education.ie/en/The-Department/Data-Protection/Information.html

PDST Technology in Education https://www.pdsttechnologyineducation.ie

Cyber Security Centre (Ireland) https://www.ncsc.gov.ie/

Cyber Security Centre (UK) https://www.ncsc.gov.uk/

Records Retention Schedule

Christian Brothers College

Retention of Records

Schools as *data controllers* must be clear about the length of time for which personal data will be kept and the reasons why the information is being retained. In determining appropriate retention periods, regard must be had for any statutory obligations imposed on a data controller. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner. It may also be anonymised to remove any personal data. Anonymisation must be irrevocable; removing names and addresses may not necessarily be sufficient.

In order to comply with this legal requirement, CBC has assigned specific responsibility and introduced procedures for ensuring that files are purged regularly and securely and that personal data is not retained any longer than is necessary. All records will be periodically reviewed in light of experience and any legal or other relevant indications.

IMPORTANT: In all cases, schools should be aware that where proceedings have been initiated, are in progress, or are reasonably foreseeable (although have not yet been taken against the school/board of management/an officer or employee of the school (which may include a volunteer)), all records relating to the individuals and incidents concerned should be preserved and should under no circumstances be deleted, destroyed or purged. The records may be of great assistance to the school in defending claims made in later years.

WARNING: In general, the limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim and the Statue of Limitations may be different in every case. In all cases where reference is made to "18 years" being the date upon which the relevant period set out in the Statute of

Limitations commences for the purposes of litigation, the school must be aware that in some situations (such as the case of a student with special educational needs, or where the claim relates to child sexual abuse, or where the student has not become aware of the damage which they have suffered, and in some other circumstances), the Statute of Limitations **may not begin to run when the student reaches 18 years of age and specific legal advice should be sought by schools on a case-by-case basis.** In all cases where retention periods have been recommended with reference to the relevant statutory period in which an individual can make a claim, these timeframes may not apply where there has been misrepresentation, deception or fraud on the part of the respondent/defendant. In such a circumstance, the College aware that the claim could arise many years after the incident complained of and the courts/tribunals/employment fora may not consider the complainant to be "out of time" to make their claim.

Student Records	Primary	Secondary	Final disposition	Comments
Registers/Roll books	Indefinitely	Indefinitely	N/A	Indefinitely. Archive when class leaves + 2 years
State exam results	N/A	N/A	N/A	SEC responsibility to retain, not a requirement for school/ETB to retain.

Records relating to pupils/students	Primary	Secondary	Confidential shredding	Comments
Enrolment Forms	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Student transfer forms (Applies from primary to primary; from one second-level school to another)	If a form is used- Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Disciplinary notes	Never destroy	Never destroy	N/A	Never destroy
Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results)	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school).
End of term/year reports	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Records of school tours/trips, including permission slips, itinerary reports	Never destroy	Never destroy	N/A	Never destroy
Scholarship applications e.g. Gaeltacht, book rental scheme	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Garda vetting form & outcome – **STUDENTS**	N/A **as primary school pupils will not be undergoing vetting**	Record of outcome retained for 12 months.	Confidential shredding	Record of outcome retained for 12 months. School to retain the reference number and date of disclosure on file, which can be checked with An Garda Siochana in the future.

Sensitive Personal Data Students	Primary	Secondary	Final disposition	Comments
Psychological assessments	Indefinitely	Indefinitely	N/A - Never destroy	Never destroy
Special Education Needs' files, reviews, correspondence and Individual Education Plans	Indefinitely	Indefinitely	N/A	Never destroy
Accident reports	Indefinitely	Indefinitely	N/A	Never destroy
Child protection records	Indefinitely	Indefinitely	N/A	Never destroy
Section 29 appeal records	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Enrolment/transfer forms where child is not enrolled or refused enrolment	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Records of complaints made by parents/ guardians	Depends entirely on the nature of the complaint.	Depends entirely on the nature of the complaint.	Confidential shredding or N/A, depending on the nature of the records.	Depends entirely on the nature of the complaint. If it is child-safeguarding, a complaint relating to teacher-handling, or an accident, then retain indefinitely. Never destroy. If it is a complaint of a more mundane nature (e.g. misspelling of child's name, parent not being contacted to be informed of parent-teacher meeting) or other minor matter, then student reaching 18 years + 7 years (6 years in which to take a claim, and 1 year for proceedings to be served on school)

Staff Records	Primary	Secondary	Final disposition	Comments
Recruitment process 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.	✓	✓	Confidential shredding	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.
Applications & CVs of candidates called for interview	✓	✓	Confidential shredding	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.
Database of applications	✓	✓	Confidential shredding	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.
Selection criteria	✓	✓	Confidential shredding	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.
Applications of candidates not shortlisted	✓	✓	Confidential shredding	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.
Unsolicited applications for jobs	✓	✓	Confidential shredding	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.
Candidates shortlisted but unsuccessful at interview	✓	✓	Confidential shredding	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.
Candidates shortlisted and are successful but do not accept offer	✓	✓	Confidential shredding	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.
Interview board marking scheme & board notes	✓	✓	Confidential shredding	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.
Panel recommendation by interview board	✓	✓	Confidential shredding	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.

Staff personnel files (whilst in employment)	**Primary**	**Secondary**	**Final Disposition**	**Comments**

e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, records of staff training etc.			Confidential shredding. Retain an anonymised sample for archival purposes.	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Application &/CV	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Qualifications	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
References	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview: database of applications (the section which relates to the employee only)	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Selection criteria	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview board marking scheme & board notes	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Panel recommendation by interview board	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Recruitment medical	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for

				proceedings to be served on the school)
Job specification/ description	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Contract/Conditions of employment	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Probation letters/forms	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
POR applications and correspondence (whether successful or not)	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Leave of absence applications			Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Job share	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Career Break	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Maternity leave	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Paternity leave	✓	✓	Confidential shredding	

				Retain for 2 years following retirement/resignation or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).
Parental leave	✓	✓	Confidential shredding	Must be kept for 8 years - Parental Leave Act 1998 Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years.
Force Majeure leave	✓	✓	Confidential shredding	Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years.
Carers leave	✓	✓	Confidential shredding	Must be kept for 8 years - Carer's Leave Act 2001 Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years
Working Time Act (attendance hours, holidays, breaks)	✓	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school). There is a statutory requirement to retain for 3 years
Allegations/complaints	✓	✓		Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). **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.
Grievance and Disciplinary records	✓	✓		Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). **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.

Occupational Health Records	Primary	Secondary	Confidential Shredding	Comments
Sickness absence records/certificates	✓	✓	Confidential shredding Or do not destroy.	Re sick leave scheme (1 in 4 rule) ref DES C/L 0060/2010 Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), 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.
Pre-employment medical assessment	✓	✓	Confidential shredding Or do not destroy?	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), 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.
Occupational health referral	✓	✓	Confidential shredding Or do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), 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.
Correspondence re retirement on ill-health grounds	✓	✓	Confidential shredding Or do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), 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.
Accident/injury at work reports	✓	✓	Confidential shredding	Retain for 10 years, or the duration of the employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), whichever is the greater (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).
Medical assessments or referrals	✓	✓	Confidential shredding Or do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless Medmark assessment 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.
Sick leave records (sick benefit forms)	✓	✓	Confidential shredding	In case of audit/refunds, Current year plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)

Superannuation /Pension /Retirement records	Primary	Secondary	Final Disposition	Comments
Records of previous service (incl. correspondence with previous employers)	✓	✓	N/A	DES advise that these should be kept indefinitely.
Pension calculation	✓	✓	Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)
Pension increases (notification to Co. Co.)	✓	✓	Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)
Salary claim forms	✓	✓	Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)

Government returns	Primary	Secondary	Final disposition	Comments
Any returns which identify individual staff/pupils,			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.

Board of Management Records	Primary	Secondary	Final disposition	Comments
Board agenda and minutes	✓	✓	N/A	Indefinitely. These should be stored securely on school property
School closure	✓	✓		On school closure, records should be transferred as per Records Retention in the event of school closure/amalgamation. A decommissioning exercise should take place with respect to archiving and recording data.
Other school-based reports/minutes	**Primary**	**Vol Sec.**	**Final disposition**	**Comments**
CCTV recordings	✓	✓	Safe/secure deletion.	28 days in the normal course, but longer on a case-by-case basis e.g. where recordings/images are requested by An Garda Síochána as part of an investigation or where the records /images capture issues such as damage/vandalism to school property and where the images/recordings are retained to investigate those issues.
Principal's monthly report including staff absences	✓	✓	N/A	Indefinitely. 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".
Financial Records	**Primary**	**Vol Sec.**	**Final disposition**	**Comments**
Audited Accounts	✓	✓	n/a	Indefinitely
Payroll and taxation	✓	✓		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.
Invoices/back-up records/receipts	✓	✓	✓	Retain for 7 years

Promotion process	Primary	Secondary	Final Disposition	Comments
Posts of Responsibility	✓	✓	N/A	Retain indefinitely on master file as it relates to pay/pension etc. (See DES guidelines)
Calculation of service	✓	✓	N/A	Retain indefinitely on master file
Promotions/POR Board master files	✓	✓	N/A	Retain indefinitely on master file
Promotions/POR Boards assessment report files	✓	✓	N/A	Retain original on personnel file in line with retention periods in "Staff Records" retention guidelines above
POR appeal documents	✓	✓	N/A	Retain original on personnel file and copy of master & appeal file. Retain for duration of employment + 7 years (6 years in which to take a claim, plus 1 year to serve proceedings on school). Copy on master and appeal file.
Correspondence from candidates re feedback	✓	✓	N/A	Depends upon nature of feedback. If feedback is from unsuccessful candidate who is not an employee within the school, keep in line with retention periods in "Staff Records" above. If feedback is from successful candidate or from unsuccessful candidate who is already an employee within the school, keep in line with "Staff personnel while in employment" above.