Coláiste Iognáid S.J.
Bóthar na Mara, Gaillimh
Tel: (091) 501550
Fax: (091) 501 551
admin@colaisteiognaid.ie

Coláiste Iognáid Data Protection Policy

The characteristic spirit of Coláiste Iognáid S.J. (the College) has at its core a desire to promote and protect the dignity of every member of its community: students, staff and parents. This includes respect for the protection of data stored at the school and for the right of access to this data. This policy is informed by the General Data Protection Regulation (EU) 2016/679. The policy applies to the Board of Management, College Management and all staff, parents/guardians, student, (including prospective students) applicants for positions within the school and service providers with access to school data. This policy sets out the manner in which personal data and sensitive personal data will be protected by the College.

DATA PROTECTION PRINCIPLES

The Board of Management is a *data controller* of *personal data* relating to its past, present and future staff, students, parents/guardians and other members of the College community. As such, the college is obliged to comply with the principles the General Data Protection Regulation (EU) 2016/679 which can be summarised as follows:

- **Obtain and process *Personal Data* fairly, lawfully and in a transparent manner**: Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the College holds on other individuals (members of staff, individuals applying for positions within the College, parents/guardians of students etc.), the information is generally furnished by the individuals themselves as a part of the contractual agreement on the understanding that the school requires such information to carry out its legitimate role as an employer and as a provider of education services to the pupils seeking to be enrolled and once they are enrolled. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.

- **Keep it only for one or more specified and explicit lawful purposes**: The College will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.

- **Process it only in ways compatible with the purposes for which it was given initially**: Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

- **Keep *Personal Data* safe and secure**: Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the College premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

- **Keep Personal Data accurate, complete and up-to-date**: Students, parents/guardians, and/or staff should inform the College of any change which the College should make to their personal data and/or sensitive

personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the College will make all necessary changes to the relevant records.

- **Ensure that it is adequate, relevant and not excessive**: Only the necessary amount of information required to provide an adequate service will be gathered and stored.

- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given**: As a general rule, the information will be kept for the duration of the individual's time in the College. Thereafter, the College will comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student. In the case of members of staff, the College will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The College may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law. See Appendix 1: Data Retention

- **Provide a copy of their *personal data* to any individual, on request**: Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

PURPOSE OF THE POLICY

Coláiste Iognáid has a legal responsibility to comply with the General Data Protection Regulation (EU) 2016/679 and takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data.

The College also has other legal obligations to comply with that involves the collection, retention, and dissemination of personal data

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the College relating to the progress of the student in their education

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

- 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 the College 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 College must record the attendance or non-attendance of students registered at the College on each school day

- Under Section 28 of the Education (Welfare) Act, 2000, the College may supply *Personal Data* kept by it to certain prescribed bodies such as the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education.

- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the College is required to furnish to the National Council for Special Education and the appropriate S.E.N.O. such information as the Council may from time to time reasonably request

- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a

school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body

- Under Section 26(4) of the Health Act, 1947 a school shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection

- Under *Children First: National Guidance for the Protection and Welfare of Children* (2017) published by the Department of Children & Youth Affairs, the Board of Management and all 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) and/or An Garda Síochána in the event of knowledge or belief of a serious crime having been committed against a child or vulnerable person.

DATA PROTECTION TERMS

In order to properly understand the College's obligations, there are some key terms which should be understood by all relevant College staff:

Data means information in a form that can be processed. It includes both *automated data* (e.g. electronic data) and *manual data*. *Automated data* means any information on computer, or information recorded with the intention that it be *processed* by computer. *Manual data* means information that is kept/recorded as part of a *relevant filing system* or with the intention that it form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.

Personal Data including sensitive data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller i.e. the college

Data Controller for the purpose of this policy is the Board of Management of Coláiste Iognáid S.J.

PERSONAL DATA COLLECTED AND RETAINED

The *Personal Data* records held by the College **may** include:

Staff records:

Categories of staff data: As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details, PPS number
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their College duties

- Records of any reports the College (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).
- The purpose of this records is the management and administration of the College and comply with the obligations set down by appropriate external agencies (such as D.E.S. payroll) and to comply with the College's obligations as an employer. Relevant data is passed onto the relevant government agencies for tax and social security reasons. Relevant data is passed onto the school's pension and life assurance providers for the purposes of those schemes. The following list includes examples of such organisations but is not exhaustive: Department of Education and Skills, Insurance Company, Revenue Commissioners.
- The basis for the collection and retention of such data is Article 9(2b) GDPR.
- Staff records are kept in the Principal Office, the Bursar's Office, and the Secretary's Office. Manual records are kept in secure filing cabinets in locked offices.
- Coláiste Iognáid 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.
- See Appendix 2 for retention periods

Students' records:

Categories of student data: These **may** include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the College. These records may include:
    - name, address and contact details, PPS number
    - date and place of birth
    - names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
    - religious belief
    - whether they (or their parents) are medical card holders
    - whether English is the student's first language and/or whether the student requires English language support
    - any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student, Psychological, psychiatric and/or medical assessments, attendance records, photographs and recorded images of students (including at College events and noting achievements), academic record – subjects studied, class assignments, examination results as recorded on official College reports, whether the student is exempt from studying Irish, records of disciplinary issues/investigations and/or sanctions imposed, Garda vetting outcome record (where the student is engaged in work experience organised with or through the College which requires that they be Garda vetted)
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the College (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).
- The purpose of such records is legislative and administrative.
- Photographs and recorded images of students are taken to celebrate College achievements, compile the Newsletter, record College events on the website and College's Twitter feed, and as part of the requirements for the New Junior Certificate Programme.
- To ensure that the student meets the College's admission criteria and meet the minimum age requirements for their course

- To furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other schools etc. in compliance with law and directions issued by government departments.
- Student personal data collected by the College is stored in the Principal's Office, Deputy Principal's Office, Coordinator of Learning Support, Career Guidance Office, and Secretary's Office. Records are also kept electronically on College computers, Eportal, PPOD (D.E.S). Manual records are stored in locked filing cabinets in locked offices.
- Data is shared with appropriate agencies as required by law. These agencies will use this data for their own established purposes. The College is not responsible for how data it is legally obligated to share with government and state agencies is used.
- See Appendix 2 for retention periods though generally personal data is retained for 7 years following the student's majority (18h year)

Board of Management Records:

Categories of Board of Management data: These **may** include:

- Name, address and contact details of each member of the Board of Management (including former members of the board of management)
- Records in relation to appointments to the Board
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals
- Garda Vetting Forms
- To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.
- Board of Management records are kept in a secure cabinet in the Principal's Office. Electronic files are stored on the Principal's password protected computer.
- Relevant data on the Finance Sub-Committee of the Board of Management minutes is passed onto the College Auditors.
- See Appendix 2 for retention periods

Parents' Records:

- The College may hold some or all of the following information about parents and/or guardians of pupils: Names and addresses of parents/legal guardians and their contact details (including any special arrangements with regard to guardianship, custody or access) and place of work; religious belief; financial information and fees related correspondence.
- The purpose of such records include: contact in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events etc., to enable the College to manage financial affairs, to manage our business for our legitimate interest, to plan the College's future, and for collection of fees and charges

Parents' Council

- The Parents' Council communicate with the parent body and school community through the College administration except where parents have given the College permission to pass on their contact details to the Parents' Council.

Providers of Services:

- The School engages many service providers throughout the course of the school year. Information retained from such service providers include contact details, bank details, PPS numbers, tax details, and invoices.

- The purpose of this information is to ensure the efficient management and administration of the College and the payments of debts.
- Financial data will be shared with the Revenue Commissioners were necessary, College Auditors, and the Finance Sub-Committee of the Board of Management.
- Data is stored in the Bursar's Office in a secure filling cabinets in locked offices.
- See Appendix 2 for retention periods.

CCTV images/recordings

- CCTV surveillance is intended for the purposes of: Protecting the school buildings and school assets, both during and after school hours; promoting the health and safety of staff, pupils and visitors; preventing bullying; reducing the incidence of crime and anti-social behaviour (including theft and vandalism); supporting the Gardaí in a bid to deter and detect crime; assisting in identifying, apprehending and prosecuting offenders; and ensuring that the school rules are respected so that the school can be properly managed.
- Cameras are located throughout the College grounds.
- Access to images/recordings is restricted to the Principal, Deputy Principals, and IT coordinator. Hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to the General Data Protection Regulation (EU) 2016/679.
- CCTV images/recordings may be passed to An Garda Síochána and parents/guardians where deemed appropriate.
- See Appendix 2 for retention periods
-

DATA SUBJECT'S RIGHTS

- Data in this school will be processed in line with the rights of individuals as data subjects (Articles 12-23 of GDPR) and these rights are as follows:
- The right to have personal information processed in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- The right to be informed, this means that the College needs to tell you what data we are using, why we are using it and for what purpose as well as informing you of the details of any third parties in receipt of data from the College.
- The right of access, you are allowed to see what data of yours we are processing if you request that from us.
- The right of rectification, that means if the data we are using is incorrect we have to correct it.
- The right to be forgotten, this means that we do not keep the data for a period longer than is necessary for the reason that it was originally collected. It also means that you have the right to issue a request to us requesting the erasure of your personal data. However, in many cases, the College will have overriding legitimate grounds for continued processing and will be unable to comply with such a request. This will be handled on a case by case basis, for further details please contact the College directly.
- The right to restrict processing, this means that you can ask us to stop using your data unless the College has a legitimate lawful purpose for continuing to do so.
- The right to object, this means that you can object to the use of your data by the College and the College must stop using it unless it has an over-riding legitimate or legal obligation to continue.

DATA REQUESTS

- Under Article 15 of the GDPR, an individual has the right to be informed whether the school holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept.
- Prior to complying with a Subject Access Request, we require proof of the applicant's identity and address to ensure that personal information is not given to the wrong person. Information requested will be provided by the College within one month of the identity of the individual of the data subject being verified. In the normal course of events, the College is obliged to respond to your access request within one month of receiving the request. In certain limited circumstances, the one month period may be extended by two months (taking into account the complexity of the request and the number of requests). Where the College is extending the period for replying to your request, it must inform you of any extension, and the reason(s) for the delay in responding, within one month of receiving the request.
- There is no fee payable by you to make an access request - the College will deal with your request for free. However, where the College believes a request is manifestly unfounded or excessive (for example where an individual makes repeated unnecessary access requests), the College may either charge a fee taking into account its administrative costs in dealing with the request(s), or refuse to act on the request(s).
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the College refuse to furnish the data to the applicant.
- Article 15 of the GDPR also provides that the right to obtain a copy of personal data must not adversely affect the rights and freedoms of others. For example, the College will not provide the requestor with personal data relating to a third party that would reveal the third party's identity.
- Any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the College over the phone. In particular the employee should: Check the identity of the caller to ensure that information is only given to a person who is entitled to that information, suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified, or refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.
- Requests for information from State bodies regarding psychological and behavioural reports must be in writing and include a statement that parental/guardian approval is given for such a request.

ROLES AND RESPONSIBILITIES

The board of management is the data controller and the principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities. The following personnel have responsibility for implementing the Data Protection Policy:

Name	Responsibility
Board of Management	Data Controller
Principal	Implementation of Policy and Data Protection Officer
Teaching Personal	Awareness of Policy
Administrative Personal	Security, Filing, and Confidentiality
I.T. Personal	Security, encryption, and confidentiality

DATA USE

Personal data is at often at the greatest risk of loss, corruption, or theft when it is being used or accessed: To mitigate this risk:

1) When working with personal data, all personnel will ensure that the screens of their computers/tablets/apps are always locked when left unattended.
2) Personal data shared by email will be downloaded, stored securely, and then deleted, i.e., such as vetting disclosures or CV's relating to Job interviews or PME placement requests
3) Data will be encrypted before being transferred electronically where appropriate.
4) Staff will not save copies of personal data to their own computers.

SANCTIONS AND DISCIPLINARY ACTION

Given the serious consequences that may arise the Board of Management of Coláiste Iognáid may invoke appropriate disciplinary procedures for failure to adhere to the school's policy on Data Protection.

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.

DATA ERASURE AND DISPOSAL

When documentation or computer files containing personal data are no longer required, the information will be disposed of carefully to continue to ensure the confidentiality of the data.

When the purpose for which the information was obtained has ceased and personal information is no longer required, the data will be deleted or disposed in a secure manner according to Records Retention Schedule (see Appendix 2).

Paper-based files and information no longer required, will be safely disposed of in shredding receptacles. Usually the data will be shredded on site by school personnel – but occasionally a third party data destruction specialist will be employed.

In the case of personal information held electronically, temporary files containing personal information will be reviewed regularly and deleted when no longer required.

When personal data reaches the point where the retention period has expired, the information will also be securely deleted and removed. In the event that IT equipment containing personal data is no longer required, all data stored on the devices will be removed prior to disposal.

Unsolicited hard copies of CV's (for Employment or PME placement) or CV's of persons replying to a job who are not shortlisted for interview will be shredded after 1 year. Electronic versions will be deleted after being downloaded to Principal's computer.

SUBJECT ACCESS REQUEST (S.A.R.) PROCEDURE

The General Data Protection Regulation (EU) 2016/679 provide for a right of access by an individual data subject to personal information held by the College. A person seeking information, the Data Subject, is required to familiarise himself/herself with this policy. This may apply to a staff member or student seeking information on his or her own behalf or maybe a parent/guardian seeking information on behalf of his or her own son. No information will be supplied that relates to another individual. Although from time to time an individual may request by telephone details of some elements of their personal data, formal SARs must be submitted in writing by post.

STUDENT DATA REQUEST

1) A student aged eighteen years or older (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.

2) If a student aged eighteen years or older has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.

3) 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 suggested that:

- If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
- If the information is of a sensitive nature, parental/guardian consent will be sought before releasing the data to the student
- If the information would be likely to be harmful to the individual concerned, parental/guardian consent will be sought before releasing the data to the student.
- Each student request for Access to Personal Data will be assessed individually.
- Where a parent/guardian makes an access request on behalf of his/her son or daughter (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 son or daughter, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the student is registered on the school's records and will be addressed to the son or daughter subject to the provisions above.

DATA REQUEST PROCEDURES

1. The Data Subject applies in writing requesting access to his/her data. The school reserves the right to request official proof of identity (e.g. photographic identification such as a passport or driver's licence) where there is any doubt on the issue of identification
2. On receipt of the Data Access Request, the Principal will check the validity of the access request and check that sufficient information to locate the data requested has been supplied. It may be necessary for the Principal to contact the data subject in the event that further details are required with a view to processing the access request.
3. The Principal will log the date of receipt of the valid request and keep a note of all steps taken to locate and collate the requested data.
4. The Principal will ensure that all relevant manual files and computers are checked for the data in respect of which the access request is made.
5. The Principal will ensure that the information is supplied promptly and within one month of first receiving the request.
6. If data relating to a Third Party is involved, it will not be disclosed without the consent of that Third party or alternatively the data will be anonymised in order to conceal the identity of the third party. Where it is not possible to anonymise or conceal the identity of the third party the data to ensure that the Third Party is not identified, then that item of data may not be released.
7. Where a school may be unsure as to what information to disclose, the school reserves the right to seek legal advice.
8. The Principal will ensure that the information is provided in an intelligible form (e.g. codes explained) where possible.
9. The documents supplied will be numbered where appropriate.

10. The Principal will sign off on the data supplied.
11. The school reserves the right to supply personal information to an individual in an electronic format e.g. on USB etc.
12. Where a subsequent or similar access request is made after the first request has been complied with, the school has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.

APPEALING A DECISION IN RELATION TO A DATA REQUEST REFUSAL

The Board of Management of the College is respectful of the right of the Data Subject to appeal a decision made in relation to a request for data from the school. To appeal a decision, the Data Subject is advised to write to or email the Data Protection Commissioner explaining the case:

Canal House, Station Road, Portarlington, Co. Laois or info@dataprotection.ie

The correspondence should include

- The name of the school
- The steps taken to have concerns dealt with
- Details of all emails, phone calls, letters between the Data Subject and this school.

DATA BREACHES

A data breach is an incident in which personal data has been lost, accessed, and/or disclosed in an unauthorised fashion. This would include, for instance, loss or theft of a laptop containing staff or student details, an email with personal information being sent to the wrong recipient, as well as more organised incidents of external hacking. All school personnel have a responsibility to take immediate action if there is a data breach.

- If a staff member suspects at any time and for any reason that a breach may have occurred, then there is a need to report it to the DPO/Data Controller as an urgent priority
- Once notification of an actual or suspected breach has been received, the DPO/Data Controller will put the Data Breach Procedure into operation with immediate effect.

The purpose of the Data Breach Procedure here below, is to ensure that all necessary steps are taken to:

1) Contain the breach and prevent further loss of data.

2) Ensure data subjects affected are advised (where necessary).

3) Comply with the law on reporting the incident to the Data Protection Commissioner if necessary.

4) Learn from the incident - identify what measures can and should be put into place to prevent similar occurrences in the future.

MONITORING THE IMPLEMENTATION OF THE POLICY

The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on students, staff and others in the College community. The implementation of the policy shall be monitored by the Principal, who as Secretary to the Board of

Management will report on its implementation to the Board. One annual report should be issued to the Board of Management to confirm that the actions/measures set down under the policy are being implemented.

Chair of the Board of Management

15/5/2025

Date

Appendix 1

Privacy Notice to Students (and their parents/guardians)

By enrolling in and attending Coláiste Iognáid S.J. you acknowledge that your personal data (including special category personal data) shall be processed by Coláiste Iognáid S.J.

This Privacy Notice gives you some helpful information about who we are, what personal data we collect about you, why, who we share it with and why, how long we keep it, and your rights.

If you need more information, please see our Data Protection Policy available at www.colaisteiognaid.ie

1. Who we are:

We are Coláiste Iognáid S.J.

Our address and contact details are Sea Road, Galway

We provide secondary level education

For further information, our Data Protection Policy available www.colaisteiognaid.ie

2. The information we collect about you

When you are a student with Coláiste Iognáid S.J. we collect and use your personal data.

The personal data we collect can include information about your identity and contact details; images/photo (including CCTV); family details; admission/enrolment details; previous schools; academic progress; PPS number; special educational needs; nationality; language; religion; medical data; information about behaviour and attendance; information about health, safety and welfare; financial information (re fees, grants, scholarships etc.); and other personal data.

Further details of the data we collect about you can be found in our Data Protection Policy.

If you are under 18 years when you enrol, we collect the name, address, contact details and other information about your parents/guardians. If you are under 18 years, your parent/guardian is consulted and asked to give consent for certain things like taking your photograph, going on school trips etc.

3. How we use your information and the legal basis

We use your personal data for purposes including:

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

For further information on what data we collect, why we collect it, how we use it, and the legal basis for same, please go to our Data Protection Policy available at www.colaisteiognaid.ie

4. Who we share your information with

We share your personal data with third parties, including other Government bodies.

This includes the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, An Garda Síochána, HSE, the Department of Social Protection, the Revenue Commissioners etc.

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

5. We do not transfer your personal data to a third country or international organisation.

6. We do not engage in automated decision making/profiling.

7. How long we hold your data

Some personal data is only kept for a short period (e.g. we will destroy at the end of an academic year because it is no longer needed). Some data we retain for a longer period (e.g. retained after you leave or otherwise finish your studies with us. For further information on the retention periods, please go to Appendix 2 0f our Data Protection Policy.

8. You have the following statutory rights that can be exercised at any time:

(a) Right to complain to supervisory authority.
(b) Right of access.
(c) Right to rectification.
(d) Right to be forgotten.
(e) Right to restrict processing.
(f) Right to data portability.
(g) Right to object and automated decision making/profiling.

For further information, please see our Data Protection Policy available on the College website

9. Contact

If you would like to discuss anything in this privacy notice, please contact the Principal in writing at admin@colaisteiognaid.ie

Record Retention Schedule

Student Records	**Final disposition**	**Comments**
Registers/Roll books	N/A	Indefinitely. Archive when class leaves + 2 years
State exam results	N/A	SEC responsibility to retain, not a requirement for school/ETB to retain.
Records relating to pupils/students	**Confidential shredding**	**Comments**
Enrolment Forms	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	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	N/A	Never destroy
Results of in-school tests/exams	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	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	N/A	Never destroy
Garda vetting form & outcome - **STUDENTS**	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	**Final disposition**	**Comments**
Psychological assessments	N/A	Never destroy
Special Education Needs' files, reviews, correspondence and Individual Education Plans	N/A	Never destroy
Accident reports	N/A	Never destroy
Child protection records	N/A	Never destroy
Section 29 appeal records	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	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).

not enrolled or refused enrolment		
Records of complaints made by parents/ guardians	Depends on the nature of the complaint.	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	**Final disposition**	**Comments**
Recruitment process		
Unsolicited CVs and PME applications	Confidential shredding	12 months from time of receipt.
Applications & CVs 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.
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.
Selection criteria, interview notes and marking schemes	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.
Staff personnel files (whilst in employment)	**Final Disposition**	**Comments**
Can include original application, CV, in-service training, applications for leave etc., contract of employment, disciplinary notes, interview notes, recruitment medical, POR applications	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)
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	ETB one doesn't have a time period advised	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	**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.
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)
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	**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	**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	**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.
Financial Records	**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.
Invoices/back-up records/receipts	Confidential Shredding	Retain for 7 years

Appendix 3

Date issued to data subject: _____ (College use only)

Access Request Form: Request for a copy of Personal Data under the Data Protection Act 1988, Data Protection (Amendment) Act 2003, and the General Data Protection Regulation 2018.

Full Name	
Name as used when in school	
Address	
Contact number	Email addresses

Students over 18 ☐	Parent/Guardian of student ☐	Former Student ☐	Current Staff ☐	Former Staff ☐
Age: Class:	Name of Student:	From: To:		From: To:

I _____ wish to be informed whether or not Coláiste Iognáid holds personal data about me/my child and to be provided with a description of this data and to be informed of the purpose for holding such data. ☐

OR

I, _____ wish to make an access request for a copy of any personal data that Coláiste Iognáid holds about me/my child. ☐

Any other information relevant to your access request (e.g. if requesting images/recordings made by CCTV, please state the date, time and location of the images/recordings (otherwise it may be very difficult or impossible for the school to locate the data).

Important: Date Access Request Forms can be presented in person to the College Administration along with Proof of Identity (e.g. official/State photographic identity document such as driver's licence, passport). Data Access Request Forms received by post must be accompanied by Garda certification of proof of identity (Once verified, Proof of Identity documentation is not retained and will be shredded). Data Access Requests must be posted to The Principal, Coláiste Iognáid, Sea Road, Galway.

Signed: _____

Date: _____

Checklist: Have you:

Completed the Access Request Form in full? ☐

Included a photocopy/certified copy of official/State photographic identity document (Driver's licence, passport etc.). ☐