

Coláiste Choilm Tullamore



Data Protection Policy

Introductory Statement

The Data Protection Policy of Coláiste Choilm, Tullamore sets out the manner in which personal data on staff, students and other individuals (e.g. parents, members of Board of Management etc.) is kept and how the data concerned is protected. This Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988, 2003 and the General Data Protection Regulation (GDPR). In this policy document the term 'parent' is taken to include 'guardian'.

The policy applies to all school staff, the Board of Management, parents, students and others (including prospective or potential students and their parents and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation, including requirements under the GDPR regulation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

The Data Privacy Statement of Colaiste Choilm, Tullamore sets out the following:

- Name of School
- Reasons why the information/data is being gathered
- How the data will be used?
- Who this data will be shared with
- The legal basis for processing the data
- How long this data will be retained?
- The right of complaint, if an individual is unhappy about the implementation of these provisions
- The individual's rights in relation to their personal data (e.g. access to data, rectification of data etc.).

The policy was formulated between February and May 2019 by a Policy Review Working Group on the staff, in consultation with the Principal, Staff, Student Council and Parents' Council.

Scope

The policy applies to the keeping and processing of personal data, both in manual form and on computer, including personal data held on both school staff and students. Coláiste Choilm recognises that individuals have a number of rights in relation to their personal information – i.e. personal data – and these rights have been enhanced by the General Data Protection Regulation (GDPR). The purpose of this policy is to assist the school in meeting its statutory obligations, to explain those obligations, and to inform staff, students and their parents how their data will be treated.

Data: means information in a form which can be processed. It includes automated data (information on computer or information recorded with the intention of putting it on computer)

and manual data (information that is kept as part of a relevant filing system, or with the intention that it should 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 and easily accessible.

Personal data: means data relating to a living individual who is or can be identified 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 school.

Data Controller: A data controller is the individual or legal entity which controls the contents and use of personal data. Coláiste Choilm, Tullamore can be considered to be the data controller, with the Principal acting for the Board of Management in exercising the functions involved.

Sensitive Personal Data: refers to *Personal Data* regarding a person's

- racial or ethnic origin, political opinions or religious or philosophical beliefs
- membership of a trade union
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence or
- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

The Policy takes cognisance of the following:

- A Guide for Data Controllers – Data Protection Commissioner
- Data Protection Act, 1988
- Data Protection (Amendment) Act, 2003
- Education Act, 1998
- Education (Welfare) Act, 2000
- The General Data Protection Regulation (GDPR), effective from 25th May 2018.

Rationale and Legal Obligations of the School

- a. Schools are legally obliged to comply with the Data Protection Act, 1988, the Data Protection (Amendment) Act, 2003 (henceforth referred to as the Data Protection Acts) and the General Data Protection Regulation (GDPR) which is a regulation in EU law on data protection and privacy for all individuals within the European Union. It also addresses the export of personal data outside the EU
- b. Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of eighteen years, must be given access to records kept by the school relating to the progress of the student in his education.
- c. Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the school.

- d. Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring.
- e. Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day.
- f. Under Section 28 of the Education (Welfare) Act, 2000, the data controller may supply personal data kept by him or her, or information extracted from such data, to the data controller of another prescribed body if he or she is satisfied that it will be used for a 'relevant purpose' only. Prescribed bodies includes the Department of Education and Skills, the State Examinations Commission, TUSLA, the Child and Family Agency, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education.
- g. Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers ('SENOs') such information as the Council may from time to time reasonably request.
- h. 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.
- i. Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of students attending the school) to be given to a health authority who has served a notice on it of medical inspection.
- j. Under Children First: National Guidance for the Protection and Welfare of Children (2011) published by the Department of Children and Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As increasing amounts of data are generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individuals' personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the Principal and Board of Management to make decisions in respect of the efficient running of the school.

Relationship to the Characteristic Spirit of the School

Coláiste Choilm aims to prepare all of our boys for the challenges, responsibilities and experiences of adult life. All members of the school community – students, parents, teachers and other staff – are held in very high regard and their dignity, worth and individuality is respected. We strive to build a sense of community based on Christian values. The school's Code of Behaviour acknowledges this and aims to promote a culture of respect throughout the school. It recognises that good discipline enables good teaching and allows good learning to take place. As part of the maintenance of the characteristic spirit of the school, we are committed to respecting the privacy and data protection rights of students, staff, parents and others who interact with us. The school wishes to achieve these aims while fully respecting individuals' rights to privacy and their rights under GDPR.

Goals/Objectives

1. To ensure that the school complies with the Data Protection Acts and GDPR.
2. To ensure compliance by the school with the eight principles of data protection as set down by the Data Protection Commissioner based on the Acts and GDPR (see below).
3. To ensure that the data protection rights of students, staff and other members of the school community are safeguarded.

Data Protection Principles

The Data Controller (school) has key legal responsibilities (under the Data Protection Acts 1988, 2003 and GDPR) in relation to the information which is kept on computer or in manual files – this pertains to past, present and future staff, students, parents and other members of the school community. These responsibilities may be summarised in the following eight principles of data protection:

1. **Obtain and process Personal Data fairly:** Information on students is gathered with the help of parents and staff. Information is also transferred from students' previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the school, parents of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the school. All such data is treated in accordance with the Data Protection Acts, GDPR and the terms of this Data Protection Policy. The information will be obtained and processed fairly.
2. **Keep it only for one or more specified and explicit lawful purposes:** The school will inform individuals of the reasons we 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.
3. **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.

4. **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 protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops / iPads) are password protected before they are removed from the school 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.
5. **Keep personal data accurate, complete and up-to-date:** Students, parents, and/or staff should inform the school of any change which the school 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 school will make all necessary changes to the relevant records. The Principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change.
6. **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.
7. **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 school. Thereafter, the school 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 school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school 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. The school's Data Privacy Statement and Acceptable Use Policy outline that most data are kept for a period of no more than seven years, while materials relating to Junior Cycle Classroom Based Assessments are destroyed as soon as possible after the Subject Learning Review Meeting, in accordance with Circular 15/2017.
8. **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.

A. Details of all personal data which will be held, the format in which it will be held and the purpose(s) for collecting the data.

Personal Data: Key Measures

The personal data records held by the school may include:

A. Staff records:

(a) 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 participating in the Droichead process. These may include:

- Name, address and contact details, PPS number
- Original records of application and appointment
- Record of appointments 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 school duties
- Digital photograph for VSware and other digital recordings/images in relation to school activities, which may be used on the school's website and social media platforms
- Details of complaints and/or grievances including consultations or competency discussions, action/improvement/evaluation plans and record of progress.

Note: a record of grievances may be maintained which is distinct from and separate to individual personnel files. Records of any reports the school (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).

(b) Format: The format in which these records will be kept may include manual records (personal file within filing system), computer records (VSware data management system database) or both.

(c) Purpose for keeping staff records may include:

- the management and administration of school business (now and in the future)
- 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)
- to facilitate pension payments in the future
- human resources management
- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- to enable the school 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)

- to enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE and any other governmental, statutory and/or regulatory departments and/or agencies
 - and for compliance with legislation relevant to the school.
- (d) **Location:** In a secure, locked filing cabinet in the Principal's office that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (e) **Security:** Manual records (personal file within a relevant filing system) are stored in a locked filing cabinet. Computer records (database) are stored on the school server and are firewall and password protected. Records are accessible only by personnel authorised to use the data.

B. Student records:

(a) **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 school including:
 - name, address and contact details, PPS number
 - data and place of birth
 - names and addresses of parents and their contact details (including any special arrangements with regard to guardianship, custody or access)
 - religious belief
 - racial, ethnic or national origin
 - membership of the Traveller Community, where relevant
 - any relevant special conditions (e.g. special educational needs, health issues, whether they or their parents are medical card holders etc.) which may apply
 - whether English is the student's first language and/or whether the student (or parent, on behalf of the student) makes a request for English language support (which may only be provided subject to the resources available in the school)
- Information on previous academic record, including assessments and other records from any previous school(s) attended by the student
- Previous school name(s) and roll number
- References
- Psychological assessments, psychiatric and/or medical assessments
- Attendance Records
- Academic record and reports – subjects studied, class assignments, examination results as recorded on official school reports, standardised test reports (e.g.

Drumcondra scores, CAT4 scores, Reasonable Accommodations Assessment test scores)

- Records of disciplinary issues/investigations and/or sanctions imposed
- Whether the student is repeating the Leaving Certificate
- Language support applicant
- Whether the student is exempt from studying Irish
- Garda Vetting outcome record (where the student is engaged in work experience organised with or through the school which requires that they be Garda vetted)
- Digital recordings (e.g. photos/videos for school activities, Classroom-Based Assessments, LCVP, school promotional activities, school events, achievements, trips and tours)
- Other records e.g. records of any serious injuries/accidents etc.
- Records of any reports the school (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, 2017)

(b) Format: The format in which these records will be kept may include manual records (personal file within filing system), computer records (VSware data management system database) or both. Digital recordings (e.g. photos, videos, audio recordings) may be made on school approved devices and stored on same, or UBS/CDs/memory cards and using cloud-based technology, and stored for a period of up to seven years. Reasonable care is taken by staff to secure the safe storage of digital recordings (see Acceptable Use Policy).

(c) Purpose for keeping student records may include:

- to enable each student to develop to his full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to support the provision of religious instruction
- to enable parents to be contacted 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 meet the educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to identify students on VSware, celebrate school achievements, compile newsletters, promote the school through social media, establish a school website, record school events, conduct LCVP recorded interviews, conduct Classroom Based Assessments, and to keep a record of the history of the school. Some digital recordings may be used for educational purposes. Some digital recordings may be stored on CDs, USB or other portable school-approved devices or saved in cloud storage. Some may be used as part of Subject Learning and Review meetings to help determine appropriate descriptor awards and apply features of quality. Some images and short video clips may be used for school

promotional purposes using the school website and/or the school's official social media platforms. Reasonable care is taken by staff to secure the safe storage of digital recordings (see Acceptable Use Policy)

- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirements for their course
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/information about the student to the Department of Education and Skills, the State Examinations Commission, the National Council for Special Education, TUSLA, and other schools etc. in compliance with law and directions issued by government departments
- to administer and report to parents on standardised tests such as the Cognitive Ability Test 4 (GL Assessment)
- to furnish, when requested by the student (or their parents in the case of a student under eighteen years) documentation/information/references to third-level educational institutions and/or prospective employers
- In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the school will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent) in order to furnish a copy of same (with the consent of the student and the student's parent) to the work experience employer.

(d) Location: In a secure, locked filing cabinet in the Principal's office, Deputy Principal's office, Year Heads' office that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(e) Security: Manual records (personal file within a relevant filing system) are stored in a locked filing cabinet. Computer records (database) are stored on the school server and are firewall and password protected. Records are accessible only by personnel authorised to use the data. Access to student data in electronic format is password protected, and security of same is outlined in the school's Acceptable Use Policy.

C. Board of Management Records:

(a) 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.

(b) Format: The format in which these records will be kept may include manual records (personal file within filing system), computer records or both.

(c) Purpose for keeping Board of Management records may include:

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.

(d) Location: In a secure, locked filing cabinet in the Principal's office that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(e) Security: Manual records (personal file within a relevant filing system) are stored in a locked filing cabinet. Computer records (database) are stored on the school server and are firewall and password protected. Records are accessible only by personnel authorised to use the data.

D. Parent Records:

(a) Categories of Parent Records: These may include:

- Name, postal address, contact details
- Details of guardianship/custody and/or access orders/arrangements
- Mobile numbers available for SMS messaging
- Email addresses
- Emergency contact details
- Siblings of student

(b) Format: The format in which these records will be kept may include manual records (personal file within filing system), computer records (VSware data management system database) or both.

(c) Purpose for keeping parent records:

These records are held in order for the school to communicate with the parents of the student e.g. progress reports, absenteeism, updates to school calendar, school self-evaluation surveys, pastoral and disciplinary matters, student unexpected illness, emergencies etc.

(d) Location: In a secure, locked filing cabinet in the school office that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(e) Security: Manual records (personal file within a relevant filing system) are stored in a locked filing cabinet. Computer records (database) are stored on the school server and are firewall and password protected. Records are accessible only by personnel authorised to use the data.

E. Other Records:

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive):

Creditors:

(a) Categories of Data: the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):

- Name
- Address
- Contact details
- PPS number
- Tax details
- Bank details and
- Amount paid.

(b) Purposes: This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

(c) Location: In a secure, locked filing cabinet in the school office that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security: Manual records (personal file within a relevant filing system) are stored in a locked filing cabinet. Computer records (database) are stored on the school server and are firewall and password protected. Records are accessible only by personnel authorised to use the data.

Charity tax-back forms:

(a) Categories of Data: the school may hold the following data in relation to donors who have made charitable donations to the school:

- Name
- Address
- telephone/mobile number(s)
- PPS number
- tax rate
- signature
- the gross amount of the donation.

- (b) Purposes:** Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents' name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the school in the case of audit by the Revenue Commissioners
- (c) Location:** In a secure, locked filing cabinet in the school office that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) Security:** Manual records (personal file within a relevant filing system) are stored in a locked filing cabinet. Computer records (database) are stored on the school server and are firewall and password protected. Records are accessible only by personnel authorised to use the data.

Closed Circuit Television (CCTV) images/recordings:

- (a) Categories of Data:** CCTV is installed in the school (corridors, locker areas) as detailed in the CCTV Policy. These CCTV systems may record images of staff, students and members of the public who visit the premises.
- (b) Purposes:** Safety and security of staff, students and visitors and to safeguard school property and equipment.
- (c) Location:** Cameras are located as detailed in the CCTV Policy. Recording equipment is located in the school office.
- (d) Security:** Access to images/recordings is restricted to the Principal, Deputy Principals, Administration Staff. Recordings are retained for twenty-eight days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

Examination Results:

- (a) Categories of Data:** The school will hold data comprising examination results in respect of its students. These include class, regular class assessments, mid-term, annual, classroom-based assessments, continuous assessment, Mock-Examinations results and State Examination Results - Junior Certificate/Cycle and Leaving Certificate.
- (b) Purposes:** The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents about subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables/school self-evaluation reports. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** Manual record (personal file within a relevant filing system) are stored in a locked filing cabinet. Computer records (database) are stored on the school server and are firewall and password protected. Records are accessible only by personnel authorised to use the data.

October Returns:

- (a) **Categories of Data:** At the beginning of each academic year (and for First Year or transferring students, on enrolment) parents and students are asked to provide the school with certain information so that the school can make returns to the Department of Education and Skills (DES), referred to as 'October Returns'. These October Returns will include sensitive personal data regarding personal circumstances which are provided by parents and students on the basis of explicit and informed consent. The October Returns contains individualised data (such as an individual student's PPS number) which acts as an 'identifier' for the DES to validate the data that belongs to a recognised student. The DES also transfers some of this data to other government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection pursuant to the Social Welfare Acts, transfers to the State Examinations Commission, transfers to the Educational Research Centre, and transfers to the Central Statistics Office pursuant to the Statistics Acts. The data will also be used by the DES for statistical, policy-making and research purposes. However, the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes. The DES has a data protection policy which can be viewed on its website (www.education.ie). The DES has also published a 'Fair Processing Notice' to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (see Circular Letter 0047/2010 in the 'Circulars' section).
- (b) **Purposes:** The school completes October Returns for the purposes of complying with DES requirements to determine staffing and resource allocations and to facilitate the orderly running of the school. The October Returns are submitted to the DES electronically. The DES has their own policy governing the security of the data sent to them by all post-primary schools. The cooperation of each student and/or their parents/guardians in completing the October Returns is greatly appreciated as the school's aim is to ensure that each student is assisted in every way to ensure that he meets his full potential.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** Manual record (personal file within a relevant filing system) are stored in a locked filing cabinet. Computer records (database) are stored on the school server and are firewall

and password protected. Records are accessible only by personnel authorised to use the data.

Processing in Line with Data Subject's Rights

Data in Coláiste Choilm will be processed in line with the data subject's rights. Data subjects have a right to:

- Request access to any data held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended
- Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Dealing with Data Access Requests

Under Section 3 of the Data Protection Acts and 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. The individual must make this request in writing (using the Data Request Form, Appendix 2) and the data controller will accede to the request within twenty-one days.

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

Section 4 access request: Individuals are entitled to a copy of their personal data on written request (using the Data Request Form, Appendix 2).

- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- Request must be responded to within forty days
- A fee of €5 will apply
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.
- 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 school refuse to furnish the data to the applicant.

Providing Information over the Phone

In Coláiste Choilm, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the school 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
- Refer the request to the Principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

B. Details of the arrangements in place to ensure compliance with the eight rules of data protection.

Compliance with Data Protection Rules

All personal data records held by the school are obtained, processed, used and retained in accordance with the following eight rules of data protection:

1. Information is obtained and processed fairly
2. Information is kept for one or more specified, explicit and lawful purposes
3. Information is used and disclosed only in ways compatible with these purposes
4. Information is kept safe and secure
5. Information is kept accurate, complete and up-to-date
6. Information kept is adequate, relevant and not excessive
7. Information is retained for no longer than is necessary for the purpose or purposes
8. A copy of his/her personal data is given to the individual on request.

The minimum age at which consent can be legitimately obtained for processing and disclosure of personal data under rules one and three above is not defined in the Data Protection Acts. However, guidance material published on the Data Protection Commissioner's website states the following:

'As a general rule in the area of education, a student aged eighteen or older may give consent themselves. A student aged from twelve up to and including seventeen should give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. In the case of students under the age of twelve consent of a parent or guardian will suffice.'

Note: Under Section 20 of the Education (Welfare) Act, 2000, each school principal must maintain a register with the names of all children attending that school. When a child is transferring from the school, the principal must notify the principal of the new school of any problems relating to school attendance that the child concerned had and of any other matters relating to the child's educational progress that he or she considers appropriate. Under Section 28 of the Act, schools may supply personal data, or information extracted from such data, to other schools or another prescribed body if they are satisfied that it will be used in recording the student's educational history, monitoring the student's educational progress or developing the student's full educational potential. The bodies which have been prescribed (and so can share information) under Section 28 are:

- The Minister for Education and Skills (which includes the Inspectorate and the National Educational Psychological Service (NEPS))
- The National Council for Special Education (NCSE)
- TUSLA
- Each school recognised in accordance with section 10 of the Education Act, 1998
- Each place designated by the Minister under section 10 of the Education Act, 1998 to be a centre for education.

In certain circumstances (e.g. Child Protection concern/concern that a law may have been broken) personal data will be disclosed to third parties, including the Department of Education and Skills, TUSLA, Gardaí, in legal proceedings, HSE personnel etc. Data can be disclosed when required by law. Data can generally be disclosed to an individual with consent.

- School registers and roll books are required to be kept indefinitely within the school.
- Pay, taxation and related school personnel service records should be retained indefinitely within the school.
- Where litigation may potentially arise in the future (e.g. in relation to accidents/personal injuries involving school personnel/students or accidents occurring on school property), the relevant records should be retained until the possibility of litigation ceases.

Note: The statute of limitations in relation to personal injuries is currently two years. The limitation period for other causes of action varies, but in most cases is not greater than six years. A limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim. In the case of minors, the limitation period does not begin to run until they reach their eighteenth birthday or later if the date of knowledge post-dates their eighteenth birthday. While schools may wish to draw up their own policies as to how long to retain such records, it would appear prudent not to destroy records likely to be relevant in litigation at least until the six-year limitation period has expired.

In line with the above, it is suggested that the information on student files might, as a general rule, be retained for a period of six years after the student has completed the Senior Cycle and/or reached the age of eighteen.

Data Access Procedures and Requirements

On making a data access request any individual (subject to the restrictions in Notes A and B below) about whom the school keeps personal data, is entitled to:

- a copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts apply, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
- know the purpose/s for processing the data

- know the identity (or the categories) of those to whom the data is disclosed
- know the source of the data, unless it is contrary to public interest
- where the processing is by automated means (e.g. credit scoring in financial institutions where a computer programme makes the 'decision' as to whether a loan should be made to an individual based on his/her credit rating) know the logic involved in automated decisions
- a copy of any data held in the form of opinions, except where such opinions were given in confidence.

To make an access request, you as an individual/data subject must:

- apply in writing, using the Data Access Request Form (Appendix 2), requesting access to your data under section 4 of the Data Protection Acts. The correspondence should be addressed to the Principal, Coláiste Choilm, O'Moore Street, Tullamore R35 WF97
- give any details which might be needed to help identify you and locate all the information the school may keep about you. 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
- pay an access fee of €5
- On receipt of the completed access request form, a co-ordinator will be appointed to check the validity of your access request and to check that sufficient information to locate the data requested has been supplied (particularly if CCTV footage/images are to be searched)
- In the case of a voluntary secondary school (Coláiste Choilm), the co-ordinator is the Principal. It may be necessary for the co-ordinator to contact you in the event that further details are required with a view to processing your access request
- The co-ordinator 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
- The co-ordinator will ensure that all relevant manual files (held within a relevant filing system) and computers are checked for the data in respect of which the access request is made
- The co-ordinator will ensure that the information is supplied promptly and within the advised timeframes
- Where a request is made under Section 3 of the Data Protection Acts, the following information will be supplied:
 - (i) what the school holds by way of personal information about you (or in the case of a request under section 3 made by a parent of a student aged under eighteen years, then the personal information held about that student) and
 - (ii) a description of the data together with details of the purposes for which his data is being kept will be provided. Actual copies of your personal files (or the personal files relating to the student) will not be supplied. No personal data can be supplied

relating to another individual. A response to your request will be provided within twenty-one days of receipt of the access request form and no fee will apply

- Where a request is made under Section 4 of the Data Protection Acts, the following information will be supplied within forty days and an administration fee of €5 will apply. The individual is entitled to a copy of all personal data, i.e.:
 - ✓ A copy of the data which is kept about him (unless one of the exemptions or prohibitions under the Data Protection Acts applies, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
 - ✓ Be advised of the purpose/s for processing his data
 - ✓ Be advised of the identity (or the categories) of those to whom the data is disclosed
 - ✓ Be advised of the source of the data, unless it is contrary to public interest
 - ✓ Where the processing is by automated means (e.g. credit scoring in financial institutions where a computer programme makes the 'decision' as to whether a loan should be made to an individual based on his credit rating), know the logic involved in automated decisions.
- Where a request is made with respect to examination results an increased time limit of sixty days from the date of the first publication of the results or from the date of the access request, whichever is the later will apply.
- Before supplying the information requested to you as data subject (or where the access request is made on behalf of a student aged under eighteen years, information relating to the student), the co-ordinator will check each item of data to establish:
 - ✓ If any of the exemptions or restrictions set out under the Data Protection Acts apply, which would result in that item of data not being released, or
 - ✓ where the data is 'health data', whether the obligation to consult with the data subject's medical practitioner applies, or
 - ✓ where the data is 'social work data', whether the prohibition on release applies.
- 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 the data to ensure that the third party is not identified, then that item of data may not be released.

Note A: Access requests by students

- Students aged eighteen and over are entitled to access their personal information in accordance with the Data Protection Acts.
- A parent may make a written data access request on behalf of a child where the data subject is under the age of eighteen.
- Students under eighteen years of age (i.e. age twelve to seventeen inclusive) can be given access to their personal information 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, and not suffering under any medical disability or medical condition which may impair his capacity to give consent, (e.g. a record of a test result) the student could readily be given access and give consent themselves
- ✓ if the record is of a sensitive nature, it would be prudent to seek parental consent
- ✓ if a student has some disability or medical condition that would impair his ability to understand the information, or if disclosure would be likely to be harmful to the individual concerned, parental consent should be sought

Note B: Exceptions to note

- Data protection regulations prohibit the supply of:
 - ✓ Health data to a patient in response to a request for access if that would cause serious harm to his physical or mental health. The regulations also provide that such data is to be communicated only by, or after consultation with, an appropriate 'health DATA PROTECTION POLICY, SEPTEMBER 2018 18 professional', normally the patient's own doctor
 - ✓ Personal data obtained in the course of carrying on social work if that would cause serious harm to the health or emotional condition of the data subject concerned. The regulations apply to social work carried on by Ministers, local authorities, the HSE or any other such bodies receiving financial assistance from public funds.

Important note to students making access requests

Where a student (aged under eighteen years) makes an access request, the school may inform the student that:

- (a) Where they make an access request, their parent(s) will be informed that they have done so and
- (b) A complete copy of the access request materials being furnished to the data subject by the school will also be furnished to the student's parent(s).

Important note to parents making access requests on behalf of their child

Where a parent makes an access request on behalf of their child (a student aged under eighteen 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 child, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the child is registered on the school's records and will be addressed to the child. The documentation will not be sent to or addressed to the parent who made the request. Where a parent is unhappy with this arrangement, the parent is invited to make an application to court under section 11 of the Guardianship of Infants Act 1964. This provision enables the court (on application by a guardian) to make a direction on any question affecting the welfare of the child. Where a court issues an order stating that a school should make certain information available to a parent, a copy of the

order should be given to the school by the parent and the school can release the data on foot of the court order.

- Where the school may be unsure as to what information to disclose, the school reserves the right to seek legal advice.
- The co-ordinator will ensure that the information is provided in an intelligible form (e.g. codes explained) or will provide an explanation.
- The Principal will have the documents supplied numbered and sign off on the appropriate response.
- The school reserves the right to supply personal information to an individual in an electronic format (e.g. e mail, USB, CD etc.)
- 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
- Where you as an individual data subject may seek to rectify incorrect information maintained by the school please notify the school and a Personal Data Rectification/Erasure Form will be supplied to you for this purpose (this form is available below in Appendix 3). You should however note that the right to rectify or delete personal data is not absolute. You have the right to make a complaint to the Data Protection Commissioner about a refusal. Where the school declines to rectify or delete the personal data as you have instructed, the school may propose to supplement your personal record, pursuant to section 6(1)(b) Data Protection Acts
- In circumstances where your access request is refused, Colaiste Choilm will write to you explaining the reasons for the refusal and the administration fee, if provided, will be returned. In such circumstances, you have the right to make a complaint to the Office of the Data Protection Commissioner www.dataprotection.ie Similarly, the administration access fee will be refunded to you if the school has to rectify, supplement or erase your personal data.
- Where requests are made for CCTV footage, an application must be made in writing (using the Data Access Request Form, available in Appendix 2) and the timeframe for response is within forty days. All necessary information such as the date, time and location of the recording should be given to the school to assist the school in dealing with your request. Where the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data. In providing a copy of personal data, the school may provide the materials in the form of a still/series of still pictures, a tape, disc, USB, with relevant images, print media or files transmitted via email. Other people's images will be obscured before the data is released. If other people's images cannot be obscured, then the images/recordings may not be released.
- These procedures are reviewed regularly in line with the school's commitment to its responsibilities under Data Protection requirements.

The Data Protection Acts state that the following data is exempt from a data access request:

1. Section 5 of the Data Protection Act provides that the right of access does not apply in a number of cases in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society on the other hand. Examples would include the need for state agencies (e.g. An Garda Síochána) to investigate crime effectively and the need to protect the international relations of the State.
2. Estimates of liability: Where the personal data consists of or is kept for the purpose of estimating the amount of the liability of the school on foot of a claim for damages or compensation and where releasing the estimate would be likely to prejudice the interests of the school in relation to the claim, the data may be withheld.
3. Legally privileged information: The general rule is that all documentation prepared in contemplation of litigation is legally privileged. So correspondence between the school and their solicitors in relation to a case against the school should not be disclosed to the claimant pursuant to a data access request.
4. Section 4 states that the right of access does not include a right to see personal data about another individual, without that other person's consent. This is necessary to protect the privacy rights of the other person. If it is reasonable for the school to conclude that redacting or omitting the particulars identifying the third party would both conceal the identity of the third party and enable the data to be disclosed (subject to the redactions), then the data could be disclosed with such redactions. However, if it is not possible to redact or omit the particulars which identify a third party, then the affected data should not be released to the applicant.
5. Section 4 also states that where personal data consists of expressions of opinion about the data subject made by another person, the data subject has a right to receive that expression of opinion except where that expression of opinion was given in confidence, and on the clear understanding that it would be treated as confidential.
6. The obligation to comply with an access request does not apply where it is impossible for the school to provide the data or where it involves a disproportionate effort.

Where a school refuses to hand over some or all of the personal data they hold in relation to a data subject (on the basis of any of the exemptions or prohibitions set out above), the school must advise the data subject of this in writing, setting out reasons for the refusal and notifying the data subject that he has the right to complain to the Office of the Data Protection Commissioner about the refusal.

Links to related school policies

The school policies of Colaiste Choilm are consistent with one another, within the context of the overall School Plan. Relevant school policies already in place or being developed or reviewed shall be examined with reference to the Data Protection Policy, and any implications which it has for them shall be addressed.

The following policies take cognisance of this Data Protection Policy:

- Acceptable Use Policy (ICT)
- Admissions/Enrolment Policy
- Anti-Bullying Policy
- CCTV Policy
- Child Safeguarding Statement
- Code of Behaviour
- Critical Incident Management Policy
- Guidance Plan
- SPHE Policy
- Substance Use Policy

Links to curriculum delivery

- Business Studies
- Civic, Social and Political Education
- English
- Gaeilge
- Geography
- History
- Home Economics
- Leaving Certificate Vocational Programme
- Modern Foreign Languages
- Science
- Transition Year

Implementation Arrangements: Roles and Responsibilities

The Board of Management of Coláiste Choilm is the data controller and the Principal is assigned the role of co-ordinating the implementation of this Data Protection Policy and for ensuring that staff who handle or have access to personal data are familiarised with their data protection responsibilities.

School administrative staff have a key role in implementing the policy and have been provided with a copy of the policy and other relevant information. Teaching staff have been provided with

the policy, including a summary of the eight rules of data protection. The Data Protection Policy and Data Privacy Statement are available to view or download from the school website.

The following personnel have particular responsibility for implementing the Data Protection Policy:

Name	Responsibility
Board of Management	Data Controller
Principal	Implementation of the Policy
Teaching Personnel	Awareness of responsibilities, adherence to these responsibilities
Administrative Personnel	Security, confidentiality
ICT Personnel	Security, encryption, confidentiality

Ratification and Communication

- The Board of Management ratified the Data Protection Policy on 25th May 2019.
- The ratified policy will be communicated to members of the school community via the school website. Copies of the policy are available at the School Office. The Parents' Council, Student Council and staff of Colaiste Choilm will be informed of the ratification of the policy and advised to familiarise themselves with the policy content. New applications on enrolment may download the policy from the school website or obtain a copy of the policy from the School Office/Reception.
- It is important that all concerned are made aware of any changes in recording information on students, staff and others in the school community.
- Parents and students are informed of the Data Protection Policy from the time of enrolment of the student (see Appendix 1 for Data Protection Statement for inclusion on relevant forms when personal information is being requested).
- Parents are advised to familiarise themselves with all school policies, available on the school website, in advance of enrolling their child in Coláiste Choilm.

Implementation Date

The policy will apply from the date of its ratification by the Board of Management in April 2019.

Monitoring the Implementation of the Policy

The monitoring and implementation of the policy will be part of the school self-evaluation process, and the Board of Management will conduct an annual review of policy planning and confirm, or make arrangement for corrective action, that the policy is being implemented. The

implementation of the policy shall be monitored by the Principal. At least one Principal's Report to the Board of Management should confirm that the actions/measures set down under the policy are being implemented.

Reviewing and Evaluating the Policy

The policy will be reviewed at least every second year, and the operation of the policy reviewed with a view to amending it, if necessary. Ongoing review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or TUSLA), legislation and feedback from parents, students, school staff and others. The policy will be revised as necessary in the light of such review and evaluation and within the framework of school planning.

In judging the impact and effectiveness of the policy the following may be taken into account:

- Students, staff and parents are aware of the policy
- Requests for access to personal data are dealt with effectively
- Personal data records are accurate
- Personal data records are held securely
- Personal data records are retained only for as long as necessary.

Ratification of policy

This policy was ratified by the Board of Management on _____.

Date of next review: April 2021

Signed: _____ Date: _____
(Chairperson of Board of Management)

Signed: _____ Date: _____
(Principal)

Appendix 1

Data Protection Statement for inclusion on relevant forms when personal information is being requested

The information collected on this form will be held by Coláiste Choilm, Tullamore in manual and in electronic format. The information will be processed in accordance with the Data Protection Act, 1988 and the Data Protection (Amendment) Act, 2003 as well as the General Data Protection Regulation (GDPR), 2018.

The purpose of holding this information is for administration/to facilitate the school in meeting the student's educational needs.

Disclosure of any of this information to statutory bodies such as the Department of Education and Skills or its agencies will take place only in accordance with legislation or regulatory requirements. Explicit consent will be sought from parents, or students aged eighteen or over, if the school wishes to disclose this information to a third party for any other reason.

Parents of students, and students aged eighteen or over, have a right to access the personal data held on them by the school and to correct it if necessary.

I consent to the use of the information supplied as described.

Signed Parent: _____

Signed Student: _____

Date: _____

Appendix 2

Data Access Request Form

Request for a copy of Personal Data under the Data Protection Act 1988 and Data Protection (Amendment) Act 2003.

Date issued to data subject:

Important:

Proof of Identity must accompany this Data Access Request Form (eg. Official/State photographic identity document such as driver’s licence, passport).

A fee of €5 must accompany this Access Request Form if it is a Section 4 Data Access Request together with proof of identity (eg. Official/State photographic identity document such as driver’s licence, passport).

Full Name	
Maiden Name (if name used during your school duration)	
Address	
Contact number *	Email addresses *

* We may need to contact you to discuss your access request.

Please tick the box which applies to you:

Student <input type="checkbox"/>	Parent of Student <input type="checkbox"/>	Former Student <input type="checkbox"/>	Current Staff <input type="checkbox"/>	Former Staff <input type="checkbox"/>
Age: Year Group/Class	Name of Student	Insert year of Leaving:	Insert Years From/To:	

Section 3 Data Access Request:

I,[insert name] wish to be informed whether or not Coláiste Choilm 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. I am making this access request under Section 3 of the Data Protection Acts.

OR

Section 4 Data Access Request:

I, [insert name] wish to make an access request for a copy of any personal data that Coláiste Choilm holds about me/my child. I am making this access request under Section 4 of the Data Protection Acts.

Section 4 Data Access Request only: I attach €5

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).

Signed

Date

Checklist: Have you:

- 1) Completed the Access Request Form in full?
- 2) Included a cheque or postal order made payable to Coláiste Choilm in the amount of €5 where a Section 4 request is made? (Please do not send us €5 if you are making a request under Section 3. There is no administration charge for a Section 3 request, and if you send us a cheque, it will be returned to you).
- 3) Signed and dated the Access Request Form?
- 4) Included a photocopy of official/State photographic identity document (driver's licence, passport etc.)?

Note to school: the school should satisfy itself as to the identity of the individual and make a note in the school records that identity has been provided, but the school should not retain a copy of the identity document.

Please return this completed and signed form, with proof of identification (and the €5 fee, if applying under Section 4) to the following address:

The Principal, Coláiste Choilm, O'Moore Street, Tullamore, Co. Offaly.

Appendix 3

Personal Data Rectification/Erasure Request Form

Request to have Personal Data Rectified or Erased.
Data Protection Act 1988 and Data Protection (Amendment) Act 2003

Important: Proof of identity (eg. Official/State photographic identity document such as driver’s licence, passport) must accompany this form.

Full Name	
Address	
Contact number *	Email addresses *

* We may need to contact you to discuss your access request.

Please tick the box which applies to you:

Student <input type="checkbox"/>	Parent of Student <input type="checkbox"/>	Former Student <input type="checkbox"/>	Current Staff <input type="checkbox"/>	Former Staff <input type="checkbox"/>
Age: Year Group/Class	Name of Student	Insert year of Leaving:	Insert Years From/To:	

I,[insert name] wish to have the data detailed below which Coláiste Choilm holds about me/my child rectified / erased (delete as appropriate). I am making this access request under Section 6 of the Data Protection Acts.

Details of the information you believe to be inaccurate and rectification required OR reason why you wish to have data erased:

You must attach relevant documents as proof of correct information e.g. where a date of birth is incorrect, please provide us with a copy of the official State Birth Certificate. Please note that your right to request rectification/deletion is not absolute and may be declined by Coláiste Choilm in certain cases. You have the right to complain about this refusal to the Office of the Data Protection Commissioner.

Signed

Date

Checklist: Have you:

- 1) Completed the Personal Data Rectification/Erasure Request Form in full?
- 2) Included document/s as proof of correct information
- 3) Signed and dated the Request Form?
- 4) Included a photocopy of official/State photographic identity document (driver's licence, passport etc.)?

**Note to school: the school should satisfy itself as to the identity of the individual, and make a note in the school records that identity has been provided but the school should not retain a copy of the identity document.*

Please address and return this completed and signed form, with proof of identity to:

The Principal, Coláiste Choilm, O'Moore Street, Tullamore, Co. Offaly.