



Monaghan Collegiate School

Data Protection Policy

Template basis used to devise the policy.

Suggested steps to follow in developing and revising/updating this policy:

1	Initiate and establish structures	<ul style="list-style-type: none"> ▪ Reference the key document, A Guide for Data Controllers, which was issued to all primary and post-primary schools in 2003. ▪ Decide on who will have responsibility for putting this policy in place. ▪ Establish a co-ordinating group, if considered necessary.
2	Review and Research	<ul style="list-style-type: none"> ▪ Study relevant resource documents and legislation, including: <ul style="list-style-type: none"> • A Guide for Data Controllers – Data Protection Commissioner • Data Protection Act, 1988 • Data Protection (Amendment) Act, 2003 • Education Act, 1998 • Education (Welfare) Act, 2000 ▪ Review existing practice or policy in your school on data protection. ▪ Identify the issues that need to be addressed.
3	Preparation of draft policy	<ul style="list-style-type: none"> ▪ (The template below is designed to assist the drafting process). Each school's own context will influence the procedures adopted.
4	Circulation/ Consultation	<ul style="list-style-type: none"> ▪ Circulate the draft policy and consult the school community, with particular reference to teachers and other school staff (including secretarial staff), parents/guardians and the board of management/trustees. ▪ Amend the draft policy, as necessary, in light of the consultation process.
5	Ratification and Communication	<ul style="list-style-type: none"> ▪ Present the policy to the board of management for ratification. ▪ Make provision for circulation of the policy, or a statement of the key elements of the policy, to all staff, parents and students, including new staff and new students. ▪ Communicate the ratified policy to other members of the school community.
6	Implementation	<ul style="list-style-type: none"> ▪ Implement the provisions of the policy. ▪ Ensure that staff who handle, or have access to, personal data are fully familiar with the policy.
7	Monitoring	<ul style="list-style-type: none"> ▪ Check that the policy is being implemented (e.g. by conducting periodic audits of data protection procedures) and identify any issues arising.
8	Review, Evaluation and Revision	<ul style="list-style-type: none"> ▪ Review and evaluate the impact of the policy at a pre-determined time, taking into account feedback from the school community and other developments. ▪ Revise as necessary, in light of the review and evaluation process.



Monaghan Collegiate School

Data Protection Policy

1. Introductory Statement:

The school's data protection policy sets out, in writing, 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. The policy was adopted by the Board of Management on the 18/05/2015 and the policy has been revised in keeping with the GDPR regulations. The Principal has had the main role in updating the policy.

2. 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.

- a. 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).
- b. 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 accessible.
- c. 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.
- d. Data Controller: A data controller is the individual or legal entity which controls the contents and use of personal data. The school can be considered to be the data controller, with the principal acting for the board of management in exercising the functions involved.

3. To whom will the policy apply?

The policy applies to all school staff, the Board of Management, Board of Governors, parents/guardians, students and others insofar as the measures under the policy relate to them.

4. Rationale

- a. Schools are obliged to comply with the Data Protection Act, 1988 and the Data Protection (Amendment) Act, 2003 (henceforth referred to as the Data Protection Acts)
- b. Under Section 9(g) of the [Education Act, 1998](#), the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in his or her 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 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.
- e. 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. See Section B.3 under Key Measures below.

5. Relationship to characteristic spirit of the school

Monaghan Collegiate School has the motto, “working together so that we may flourish as individuals” where the school community seeks to prepare young people in an environment of Christian compassion to reach their individual potential in preparation for lifelong learning. The school provides for a safe learning environment based on respect for oneself and each other.

6. Goals/Objectives

The objectives are:

- a. To ensure that the school complies with the Data Protection Acts.
- b. To ensure compliance by the school with the eight rules of data protection as set down by the Data Protection Commissioner based on the Acts (see below).
- c. To ensure that the data protection rights of students, staff and other members of the school community are safeguarded.

7. Content of Policy

The policy content is divided into two sections as follows

- 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 in each case.
- b. Details of the arrangements in place to ensure compliance with the eight rules of data protection.

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 in each case

The personal data records held by the school may include:

- a. **Staff records:** These may include:
 - i. Name, address and contact details, PPS number
 - ii. Original records of application and appointment
 - iii. Record of appointments to promotion posts
 - iv. Details of approved absences (career breaks, parental leave, study leave etc.)
 - v. Details of work record (qualifications, classes taught, subjects etc)
 - vi. 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.

Format: The biographical data is held in both manual and on computer, other data is manually held.

Purpose for keeping staff records include

- facilitating the payment of staff, and pension payments in the future.
- to ensure that next of kin may be contacted in an emergency and
- to a record of promotions made and duties undertaken.

- b. **Student records:** These may include:

- a. Information which may be sought and recorded at enrolment, including:
 - i. name, address and contact details, PPS number
 - ii. names and addresses of parents/guardians and their contact details
 - iii. religious belief
 - iv. racial, ethnic or national origin
 - v. membership of the Traveller community, where relevant
 - vi. any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply
- b. Information on previous academic record
- c. Psychological assessments
- d. Attendance Records
- e. Academic record – subjects studied, class assignments, examination results as recorded on official school reports
- f. Records of significant achievements

- g. Records of disciplinary issues and/or sanctions imposed
- h. Other records e.g. records of any serious injuries/accidents etc.

Format: The biographical data, and behavioural data is held in both manual and on computer, other data is manually held.

Purpose for keeping student records include:

- to enable each student to develop his/her 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 parent/guardians to be contacted in the case of emergency etc.

- c. **Board of Management/Board of Governors records:** These may include:
 - a. Name, address and contact details of each member of the board of management, board of governors
 - b. Records in relation to appointments to the boards
 - c. Minutes of board of management/governors meetings and correspondence to the boards which may include references to particular individuals.

Format: Biographical details are kept both manually and on computer. record of contribution to meetings are kept manually in the minutes.

Purpose for keeping board of management/governors records include:

- a record of board appointments,
- documenting decisions made by the board etc.

- d. **Other Records:**
 - On parents the school will hold records
 - a. of parental address and contact numbers
 - b. school fee details and grant applications as relevant.

Format: The records will be held on the computer.

The records are held so that

- parents may be communicated with.
- invoices of monies owed to the school may be generated.

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

- a. The eight rules of Data Protection, based on the Data Protection Acts
 1. Obtain and process information fairly
 2. Keep it only for one or more specified, explicit and lawful purposes
 3. Use and disclose it only in ways compatible with these purposes
 4. Keep it safe and secure
 5. Keep it accurate, complete and up-to-date
 6. Ensure that it is adequate, relevant and not excessive
 7. Retain it for no longer than is necessary for the purpose or purposes
 8. Give a copy of his/her personal data to that individual on request.

The minimum age at which consent can be legitimately obtained for processing and disclosure of personal data under rules 1 and 3 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.”

- b. Procedures to comply with the eight rules.

1. Obtain and process information fairly.

To fairly obtain data the data subject must, at the time the personal data is being collected, be made aware of:

1. the identity of the data controller
2. the purpose in collecting the data,
3. and the persons or categories of persons to whom the data may be disclosed
4. any other information which is necessary so that processing may be fair.

To fairly process personal data

1. it must have been fairly obtained, and:
2. the data subject must have given consent to the processing or the processing must be necessary for one of the following reasons:
 - a. the performance of a contract to which the data subject is party
 - b. in order to take steps at the request of the data subject prior to entering into a contract
 - c. compliance with a legal obligation, other than that imposed by contract
 - d. to prevent injury or other damage to the health of a data subject
 - e. to prevent serious loss or damage to property of the data subject
 - f. to protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged
 - g. for the administration of justice
 - h. for the performance of a function conferred on a person by or under an enactment
 - i. for the performance of a function of the Government or a Minister of the Government
 - j. for the performance of any other function of a public nature performed in the public interest by a person
 - k. for the purpose of the legitimate interests pursued by a data controller except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

To fairly process sensitive data (see definitions) there are additional special conditions of which at least one of the following must be met:

1. the data subject has given explicit consent to the processing, i.e. the data subject has been clearly informed of the purpose/s in processing the data and has supplied his/her data with that understanding,
2. or the processing must be necessary for one of the following reasons
 - a. for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment
 - b. to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where, consent cannot be given, or the data controller cannot reasonably be expected to obtain such consent
 - c. to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld
 - d. it is carried out by a not for profit organisation in respect of its members or other persons in regular contact with the organisation
 - e. the information being processed has been made public as a result of steps deliberately taken by the data subject
 - f. for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights
 - g. for medical purposes
 - h. is carried out by political parties or candidates for election in the context of an election

- i. for the purpose of the assessment or payment of a tax liability
- j. in relation to the administration of a Social Welfare scheme.

2. Keep it only for one or more specified, explicit and lawful purposes

You may only keep data for a purpose/s that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with the purpose. An individual has a right to question the purpose for which you hold his/her data and you must be able to identify that purpose. To comply with this rule:

- a. in general the persons whose data you collect should know the reason/s
- b. why you collect and keep it
- c. the purpose for which you collect and keep the data should be a lawful one
- d. you should be aware of the different sets of data which you keep and
- e. specific purpose of each.

3. Use and disclose it only in ways compatible with these purposes

Any use or disclosure must be necessary for the purpose/s or compatible with the purpose/s for which you collect and keep the data. You should ask whether the data subject would be surprised to learn that a particular use of or disclosure is taking place. A key test of compatibility is:

- a. do you use the data only in ways consistent with the purpose/s for which they were obtained?
- b. do you disclose the data only in ways consistent with that purpose/s?

The rule, that disclosures of information must always be compatible with the purpose/s for which that information was obtained, is lifted in certain restricted cases by section 8 of the Act. Examples of such cases would include some obvious situations where disclosure of the information is required by law or is made to the individual himself/herself or with his/her consent.

4. Keep it safe and secure

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The security of personal information is all-important, but the key word here is appropriate, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorised disclosure. High standards of security are, nevertheless, essential for all personal information. The nature of security used may take into account what is available, the cost of implementation and the sensitivity of the data in question. A minimum standard of security would include the following:

- a. access to the information restricted to authorised staff on a "need-to know" basis in accordance with a defined policy
- b. computer systems should be password protected
- c. information on computer screens and manual files should be kept hidden from callers to your offices
- d. back-up procedure in operation for computer held data, including off-site back-up
- e. all reasonable measures should be taken to ensure that your staff are made aware of the organisation's security measures, and comply with them
- f. all waste papers, printouts, etc. should be disposed of carefully
- g. a designated person should be responsible for security and there should be periodic reviews of the measures and practices in place
- h. premises should be secure when unoccupied
- i. a contract should be in place with any data processor which imposes equivalent security obligations on the data processor.

5. Keep it accurate, complete and up-to-date

(While this rule applies to all computer held data and any new manual records created from July 2003, it will only apply to existing manual records from October 2007.) Apart from ensuring compliance with the Acts, this requirement has an additional importance in that you may be liable to an individual for damages if you fail to observe the duty of care provision in the Acts applying to the handling of personal data. To comply with this rule you should ensure that:

- a. your clerical and computer procedures are adequate to ensure high levels of data accuracy
- b. the general requirement to keep personal data up-to-date has been fully examined
- c. appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.

Note: The accuracy requirement does not apply to back-up data, that is, to data kept only for the specific and limited purpose of replacing other data in the event of their being lost, destroyed or damaged.

6. Ensure that it is adequate, relevant and not excessive

(While this rule applies to all computer held data and any new manual records created from July 2003 it will only apply to existing manual records from October 2007.) You can fulfil this requirement if you make sure you are keeping only the minimum amount of personal data which you need to keep to achieve your specified purpose/s. You should set down specific criteria to judge what is adequate, relevant, and not excessive and apply those criteria to each information item and the purpose/s for which it is held. To comply with this rule you should ensure that the information held is:

- a. adequate in relation to the purpose/s for which you keep it
- b. relevant in relation to the purpose/s for which you keep it
- c. not excessive in relation to the purpose/s for which you keep it.

7. Retain it for no longer than is necessary for the purpose or purposes

(While this rule applies to all computer held data and any new manual records created from July 2003 it will only apply to existing manual records from October 2007.) Nowadays information can be kept cheaply and effectively, particularly on computer. This requirement places a responsibility on data controllers to be clear about the length of time data will be kept and the reason why the information is being retained. You should assign specific responsibility for ensuring that files are regularly purged and that personal information is not retained any longer than necessary. To comply with this rule you should have:

- a. defined policy on retention periods for all items of personal data kept management,
- b. clerical and computer procedures in place to implement such a policy.

In general, personal data should not be kept for any longer than is necessary to fulfil the function for which it was first recorded. Retention times cannot be rigidly prescribed to cover every possible situation and schools need to exercise their individual judgement in this regard in relation to each category of records held. However, the following particular requirements should be met:

- a. School registers and roll books are required to be kept indefinitely within the school. Consideration is being given to amending the Data Protection Acts to allow schools to deposit completed school registers and roll books which are no longer required for administrative purposes with the Local Authority Archive Service. The Department will notify schools of any changes to the Acts in this regard.
- b. Pay, taxation and related school personnel service records should be retained indefinitely within the school.
- c. 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 18th birthday or later if the date of knowledge post-dates their 18th 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 18.

8. Give a copy of his/her personal data to that individual, on request

On making an access request any individual, about whom you keep personal data, is entitled to:

- a. a copy of the data you are keeping about him/her
- b. know your purpose/s for processing his/her data
- c. know the identity of those to whom you disclose the data
- d. know the source of the data, unless it is contrary to public interest
- e. 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.

It is important that you have clear co-ordinated procedures in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is being made.

To make an access request the data subject must:

- a. apply to you in writing give any details which might be needed to help you identify him/her and locate all the information you may keep about him/her e.g. previous addresses, customer account numbers
- b. pay you an access fee if you wish to charge one. You need not do so, but if you do it cannot exceed the prescribed amount of €6.35

Every individual about whom a data controller keeps personal information has a number of other rights under the Act, in addition to the Right of Access. These include the right to have any inaccurate information rectified or erased, to have personal data taken off a direct marketing or direct mailing list and the right to complain to the Data Protection Commissioner.

There are a number of exceptions to the general rule of Right of Access, including those specified in Notes A and B below.

Note A: Access requests by students

1. Students aged 18 and over are entitled to access their personal information in accordance with the Data Protection Acts.
2. Students under 18 years of age 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:
 - a. if the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
 - b. if the record is of a sensitive nature, it would be prudent to seek parental/guardian consent
 - c. if a student has some disability or medical condition that would impair his or her ability to understand the information, or if disclosure would be likely to be harmful to the individual concerned, parental/guardian consent should be sought.

Note B: Exceptions to note:

Schools should note that data protection regulations prohibit the supply of:

1. health data to a patient in response to a request for access if that would cause serious harm to his or her physical or mental health. The regulations also provide that such data is to be communicated only by, or after consultation with, an appropriate "health professional", normally the patient's own doctor
2. 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.

Note C. Requests regarding data

1. Requests regarding data should be made in writing to the school office and will be processed by the member of staff appointed in conjunction with the school secretary and the principal.
2. Applicants requesting information must identify themselves by photographic id. or by identification by a member of staff.
3. In the case where parents are separated, legal impairments to receiving data must be considered.
4. If spouses are separated and one of them has obtained an order for custody but both of them remain guardians, then both of them are entitled to be involved in important decisions which affect the child.
5. Information should be supplied within forty days of receiving the request, excluding school holidays.

8. Links to Other Policies and to Curriculum Delivery

Data protection policies may impinge on the operation of the following policies.

1. Child Protection Policy
2. Guidance Plan
3. Anti-Bullying Policy
4. Substance Use Policy
5. Code of Behaviour.

Information obtained and exchanged in CSPE is also subject to data protection as is information collected during Transition Year projects or LCVP projects.

9. Implementation Arrangements, Roles and Responsibilities

- a. In keeping with all policies the Principal has the main responsibility for implementing the policy.
- b. The office staff has a major role in implementing the policy on the ground.
- c. The staff coordinator has a main role in monitoring the implementation of the policy.

10. Ratification & Communication

The policy will be discussed and ratified by the Board at the September meeting.

The policy will be communicated to staff at the staff meeting where they will be taken through the 8 steps. All staff have already gone through the presentation prepared by the JMB.

11. Implementation Date

Target date for implementing the policy is 1st October 2018

12. Monitoring the implementation of the policy


The principal will monitor the implementation of the policy.

13. Reviewing and evaluating the policy

The policy should be reviewed and evaluated at certain pre-determined times and, as necessary. Ongoing review and evaluation should take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Science or the NEWB), legislation and feedback from parents/guardians, students, school staff and others. The policy should be revised as necessary in the light of such review and evaluation and within the framework of school planning.

The policy should be reviewed annually giving consideration to the following.

- Students, staff and parents/guardians 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.

	<p>Monaghan Collegiate School</p> <p>Data Protection Policy</p>
---	---


This Data Protection Policy has been tabled, considered and discussed by the Board of management of Monaghan Collegiate School and has been ratified.

Signed _____ Date ____/____/_____

Chair of the Board of management.

Appendix 1

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

	<p>Monaghan Collegiate School</p> <p>Data Protection</p> <p>Collection of Data</p>
---	---

The information collected on this form will be held by Monaghan Collegiate School 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.

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/Guardians or students aged 18 or over if the school wishes to disclose this information to a third party for any other reason.

Parents/Guardians of students and students aged 18 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/Guardian: _____

Signed Student: _____

Appendix 2 Basic Data Protection Checklist

x/v	Action
	Are the individuals whose data you collect aware of your identity?
	Have you told the data subject what use you make of his/her data?
	Are the disclosures you make of that data legitimate ones?
	Do you have appropriate security measures in place?
	Do you have appropriate procedures in place to ensure that each data item is kept up-to-date
	Do you have a defined policy on retention periods for all items of personal data?
	Do you have a data protection policy in place?
	Do you have procedures for handling access requests from individuals?
	Are you clear on whether or not you should be registered?
	Are your staff appropriately trained in data protection?
	Do you regularly review and audit the data which you hold and the manner in which they are processed?

Heading	Action Points	Date for Action	Date for Review
Data Retention and Accountability	<p>Review all personal data the school currently holds and determine whether or not it is held in accordance with the GDPR.</p> <p>Make an inventory of all personal data held by the school/ETB and examine it under the following headings:</p> <ul style="list-style-type: none"> • Why is it being held? • How was it obtained? • Why was it originally gathered? • How long will it be retained? • How secure is it, both in terms of encryption and accessibility? • Is the data ever shared with third parties and on what basis might this be done? 		
Basis for processing data	<p>Identify and document the legal basis for processing personal data.</p> <p>Draft or update the schools privacy notice to explain legal basis</p> <p>Communicate Privacy Notice to relevant stakeholders</p>		
Data Retention times	Have an up-to-date data retention schedule in place		
GDPR Obligations	Schools should familiarise themselves with their obligations under the GDPR and take steps to ensure compliance		
Training	Ensure staff are effectively trained in the new policies & procedures		

Appendix 3 Staff reference on Data Protection

The eight rules of Data Protection, based on the Data Protection Acts

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to that individual on request.