



Clonkeen College
Clonkeen Road
Blackrock
Co. Dublin

Phone - 2892709
Fax - 2898260
Email – reception@clonkeencollege.ie

DATA PROTECTION POLICY

Introductory Statement

All personal information which Clonkeen College holds is protected by the Data Protection Acts 1988 and 2018 and general data protection regulation (GDPR). The school takes its responsibilities under these laws seriously.

This policy sets out the way personal data is kept and how the data concerned is protected by Clonkeen College.

Summary

Clonkeen College is a data controller of personal data relating to its past, present, future and potential / prospective employees, students, parents, members of board of management and various other individuals.

As such, Clonkeen College is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2018 and GDPR which can be summarised as follows:

- obtain and process personal data fairly.
- keep it only for one or more specified and explicit lawful purposes.
- process it only in ways compatible with the purposes for which it was given initially.
- keep Personal Data safe and secure.
- keep data accurate, complete, and up to date.
- ensure that it is adequate, relevant, and not excessive.

- retain it no longer than is necessary for the specified purpose or purposes; and,
- provide a copy of personal data to any individual, on request.

Scope

Purpose of the Policy:

The Data Protection Acts and GDPR apply to the keeping and processing of personal data, both in manual and electronic form. The purpose of this policy is to assist Clonkeen College to meet its statutory obligations while explaining those obligations to staff.

To whom will the Policy apply?

This policy applies to all school staff, the board of management, parents/guardians, students, and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Personal data will be stored securely, so that confidential information is protected in compliance with relevant legislation.

Glossary

To properly understand the school's obligations, there are some key terms which should be understood by all relevant staff:

Data means information in a form that can be processed and stored. It includes both electronic data and manual data. Electronic data means any information transmitted, shared, or stored on computer or any form of information system, software application, or network or information recorded with the intention that it be processed, transmitted, or stored by electronic means.

Manual data means information that is recorded as part of a relevant filing system or with the intention that it form part of such a 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 accessible. Examples might include student files stored in alphabetic order in a filing cabinet or personnel files stored in the office.

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

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 criminal convictions or the alleged commission of an offence.

Rationale

Why is it necessary to devise a data protection policy at this time?

In addition to its legal obligations under the broad remit of educational legislation and other legislation, Clonkeen College has a legal responsibility to comply with the Data Protection Acts and GDPR. As more and more 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. In the absence of a documented policy, there is a risk that data entrusted to the school will be retained, used, or disclosed in ways that breach individuals' data protection rights.

Identifying Personal Data

The Personal Data records held by Clonkeen College may include:

A. Staff records:

(a) **Categories of Staff Data:** These may include:

- Name, address, and contact details,
- Date of birth, PPS number
- Marital and family status
- Educational or previous employment background
- Original records of application and appointment
- Interview records, references
- Record of appointments to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Records of in-service courses
- Details of work record (qualifications, classes taught, subjects etc)
- 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.
- Superannuation and pension documentation
- Salary, payroll details, bank details.
- Medical card details

(b) **Purposes:** For the management of Clonkeen College school business now and into the future. E.g.: to facilitate the payment of staff, to facilitate pension payments in the future, human resources management, recording promotions etc. and for compliance with legislation.

Sensitive Personal Data

Certain categories of information are categorised as sensitive under data protection legislation. Clonkeen College may hold some or all the following sensitive information about its employees:

Medical information, records of sickness absence and medical certificates. The purpose of keeping this sort of information is to administer sick pay and disability entitlement, monitor and manage sickness absence and to comply with our health and safety obligations.

Garda Vetting records will be retained in compliance with DES C/L 0063/2010 and subsequent relevant circular letters.

(c) **Location:** Staff records are kept in the offices at Clonkeen College and/or as appropriate in the storage systems and networks deployed by service providers providing the school with various electronic information and communication systems.

(d) **Security:** Clonkeen College stores personal information held in the school in controlled access databases, computers, and devices (including computerised and manual files) in offices at Clonkeen College. The school will take appropriate security measures against unauthorised access to, or alteration, disclosure, or destruction of this data and against their accidental loss or destruction. Some relevant data is stored permanently or temporarily on the storage systems and networks deployed by service providers providing the school with various electronic information and communication systems. These service providers have undertaken to ensure the security of such data from unauthorised access and to retain or delete such data on request in line with data protection legislation and GDPR.

B. Student records:

These may include:

- Information which may be sought and recorded at enrolment, including name, address and contact details, PPS number; names and addresses of parents/guardians and their contact details; religious belief; racial, ethnic or national origin; any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply.
- Information on previous academic record
- Psychological assessments
- Cognitive Abilities Tests (CATs) & Diagnostic Abilities Tests (DATs)
- Attendance Records
- Academic record – subjects studied, class assignments, examination results and associated comments as recorded on official school reports.
- Records of significant achievements
- Records of disciplinary issues and/or sanctions imposed.
- Other records e.g., records of any serious injuries/accidents etc.
- Records of student examination results and progress maintained by individual teachers.
- Data relating to Irish language exemption if applicable.

The purpose/s for obtaining and holding these records is to enable each student to develop 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 parent/guardians to be contacted in the case of emergency etc.

Each year, each recognised post primary school makes a return to the Department of Education and Skills, the data from which allow the Department of Education and Skills calculate the teaching posts and core funding to be allocated to each recognised post primary school, for the following school year. These returns are made in accordance with *The Rules and Programme for Secondary Schools* via a process called the Annual Post-Primary School October Return/Examination Entries, or more familiarly known as the October Returns.

In making their respective returns to the Department, post primary schools transfer personal data and personal sensitive data on each of their enrolled students. The only purpose some post primary schools may collect some of these data is to meet the data requirements for their October Returns to the Department. Sensitive Data which may be sought at the time of enrolment includes membership of the travelling community and medical card information. This information is sought and retained for the purpose of completion of the October Returns. Explicit permission will be sought from parents/guardians before processing this data in line with DES C/L 47/2010.

Clonkeen College also keeps records of students as detailed below:

(a) Categories of Student Data:

Records of students with Special Education Needs

The school receives and retains a copy of student Psychological Reports which may include:

- name, address, and date of birth
- PPS Number
- psychological assessment if received.
- category of assessed disability
- parent/guardian name and contact details

(b) Purposes:

For the management and administration of school business now and into the future, this will include the administration of the school's teacher allocation, special needs allocation and language support.

(c) Location:

These student records are kept in the offices at Clonkeen College and/or as appropriate in the storage systems and networks deployed by service providers providing the school with various electronic information and communication systems.

(d) Security:

Clonkeen College stores all personal information in controlled access, centralised databases (including computerised and manual files) in the offices at Clonkeen College. The school will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of this data and against their accidental loss or destruction. Some relevant data is stored permanently or temporarily on the storage systems and networks deployed by service

providers providing the school with various electronic information and communication systems. These service providers have undertaken to ensure the security of such data from unauthorised access and to retain or delete such data on request in line with data protection legislation and GDPR.

C. CCTV Images/Recordings

(a) Categories: CCTV is installed in the school externally i.e., perimeter walls/fencing and internally. 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 externally and internally. Recording equipment is located in the school offices.

(d) Security: Permission to access images/recordings must be given by the Principal and/or Deputy Principal of the school. Tapes, DVDs, hard disk recordings are retained for a period of time, except if required for the investigation of an incident.

D. School Email Accounts

- All school staff are issued a school email address.
- Always use the school email account for school business.
- The school email account is not to be used for unapproved non-school business.
- The email account provided by the school is the property of the employer and can be subject to data access requests.
- Email attachments containing personal data should be password protected.
- Be cautious about opening email attachments or links from unknown sources, if in doubt delete.

Applying the Data Protection Principles to Personal Data

The Data Protection Acts 1988 and 2018 and GDPR confer rights on individuals as well as responsibilities on those persons controlling and processing personal data. Clonkeen College has key responsibilities in relation to the information which it keeps on computer or in structured manual files about individuals. The school undertakes to execute its responsibilities in accordance with the eight Data Protection Principles/Rules as outlined below:

1. Obtain and process Personal Data fairly

Clonkeen College will ensure that data subjects (staff, students & parents) are aware, at the time the personal data is being collected, of:

- the name of the school (the “data controller”)
- the purpose in collecting the data.

- the persons or categories of persons to whom the data may be disclosed.
- whether replies to questions asked are obligatory and the consequences of not providing replies to those questions.
- the existence of the right of access to their Personal Data.
- the right to rectify their data if inaccurate or processed unfairly.
- any other information which is necessary so that processing may be fair and to ensure the data subject has all the information that is necessary to be aware as to how their data will be processed.

This will be achieved by adopting appropriate data protection notices at the point of data capture e.g., Staff Application forms, student enrolment forms. While an express signature of indication of consent is not necessarily always required, it is strongly recommended, and will be requested, where possible.

In the case of *Sensitive Personal Data* explicitly given consent will be requested unless it is necessary:

- to process the sensitive data in connection with an employment right or obligation.
- to prevent injury or other damage to the health of a person or otherwise to protect their vital interests.
- 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.
- for medical purposes (more extensive advice as to what constitutes medical purposes is available from www.dataprotection.ie)
- for the purpose of the assessment or payment of a tax liability
- in relation to the administration of a Social Welfare scheme.

The minimum age at which consent can be legitimately obtained for processing and disclosure of Personal Data is not defined in the Data Protection Acts and GDPR. However, the Data Protection Commissioner recommends, that, *“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.”*

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

Clonkeen College will keep data for purposes that are specific, lawful, and clearly stated and the data will only be processed in a manner compatible with these purposes. Management and staff will be made aware of the purpose for which data is kept and ensure that it is not used for any purpose which may be incompatible with the original purpose.

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

Clonkeen College will only use and disclose personal data in ways that are necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data. Clonkeen College will ensure that staff/departments involved in processing personal data are aware of the purpose of collecting such data and use/process it only for that specific purpose or

compatible purpose/s. For the purposes outlined above it may from time to time be necessary to disclose employee's personal information to third parties, including: the Department of Education & Skills, Revenue Commissioners, Department of Social Protection, the Central Statistics Office, the Teaching Council, An Garda Síochána, other educational institutions, banks and other financial institutions, service providers acting in the role of data processors, past and future employers, auditors, pension administrators, trade unions and staff associations or other.

Student (and/or parent/guardian) data may be disclosed to third parties including: The Department of Education and Science (which includes the Inspectorate and the National Educational Psychological Service (NEPS) & Universities/ Colleges /Institutes.

It may also be necessary to disclose information to comply with any legal obligations. Clonkeen College takes all reasonable steps as required by law to ensure the safety, privacy, and integrity of the information and, where appropriate, enter into contracts with such third parties to protect the privacy and integrity of any information supplied. Clonkeen College will endeavour to comply with Department of Finance Guidelines in relation to the transfer of data to third parties.

4. Keep it safe and secure.

Clonkeen College stores personal information held in the school in controlled access databases, computers, and devices (including computerised and manual files) in offices at Clonkeen College. The school will take appropriate security measures against unauthorised access to, or alteration, disclosure, or destruction of this data and against their accidental loss or destruction. Some relevant data is stored permanently or temporarily on the storage systems and networks deployed by service providers providing the school with various electronic information and communication systems. These service providers have undertaken to ensure the security of such data from unauthorised access and to retain or delete such data on request in line with data protection legislation and GDPR. The school acknowledges that high standards of security are essential for processing all personal information and endeavours to comply with the Department of Finance Guidelines which contains comprehensive guidelines regarding best practice in the area of data security. Some of the security measures taken include:

- Access to files containing personal data (computerised and manual) is restricted to the staff who work in that area.
- On-site computer systems are password protected and are backed up daily to a secure server.
- The school has entered into Data Processing Agreements with service providers of electronic information and communications systems regarding their responsibilities under the terms of GDPR as Data Processors of the school data transmitted and stored on their systems.
- The Offices are secured and alarmed (monitored) when not occupied.
- Wastepaper which may include personal information is confidentially shredded.
- Teachers who keep test and other data pertaining to students have been made aware of this policy and of the requirement under the Data Protection Acts and GDPR to maintain such data securely.

5. Keep it accurate and up to date.

Clonkeen College has procedures in place that are adequate to ensure high levels of data accuracy and completeness and to ensure that personal data is kept up to date. We rely on the individuals who supply personal information (staff, students, and others) to ensure that the information provided is correct and to update us in relation to any changes to the information provided. Notwithstanding this, according to the terms Data Protection Acts and GDPR, individuals have the right to have personal information corrected if necessary. If an individual feels that the information held is incorrect, they should write to the Principal.

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

Personal data held by Clonkeen College will be adequate, relevant, and not excessive in relation to the purpose/s for which it is kept. Periodic checking of data (electronic and manual) will be made to ensure that personal data held is not excessive and remains adequate and relevant for the purpose for which it is kept. Teachers who keep test and other data pertaining to students have been made aware of this requirement.

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

Clonkeen College will have a defined policy on retention periods for personal data and appropriate procedures in place to implement such a policy. In setting retention periods for different sets of data, regard will be taken of the relevant legislative requirements, the possibility of litigation, the requirement to keep an archive for historical purposes and the retention periods laid down by funding agencies. Retention times cannot be rigidly prescribed to cover every possible situation and the school will exercise judgement, taking account of statutory obligation and best practice in this regard in relation to each category of records held. However, the following requirements should be met:

- The school registers and roll books are required to be kept indefinitely within the school.
- Pay, taxation and related employment records should be retained in accordance with the time periods set out in various Acts and Statutory Instruments governing taxation and employment law.
- Where litigation may potentially arise in the future (e.g., in relation to accidents/personal injuries involving employees/students or accidents occurring on school property), the relevant records should be retained until the possibility of litigation ceases.
- Teachers who keep test and other data pertaining to students have been made aware of this requirement.

8. Give a copy of personal data to any individual, on request.

Data subjects have the right to periodically review, update and/or correct the information held about them. On making an access request any individual (subject to the restrictions in Notes A and B below) about whom Clonkeen College keeps Personal Data, is entitled to:

- a copy of the data which is kept about him/her.
- know the purpose/s for processing data.
- know the identity of those to whom the data is disclosed.
- know the source of the data unless it is contrary to public interest.
- know the logic involved in automated decisions.
- a copy of any data held in the form of opinions, except in certain limited circumstances where such expression of opinion was given in confidence or on the understanding that it would be treated as confidential.

To make an access request, an individual must:

- apply in writing to the Principal stating that an Access Request is being made under Section 4 of the Data Protection Acts 1988-2018.
- give any details which might be needed to help identify him/her and locate all the information the school may keep about him/her.
- pay an access fee if the school wishes to charge one.
- There are several exceptions to the general rule of Right of Access, including those specified in Notes A and B below.
- Teachers who keep test and other data pertaining to students have been made aware of this requirement.

9. Handling access requests

1. The Principal will be nominated as the Co-ordinator responsible for handling access requests.
2. The Co-ordinator will check the validity of the access request, check that sufficient information has been provided to definitively identify the individual and that sufficient information to locate the data has been supplied.
3. 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 data.
4. The Co-ordinator will ensure that all relevant manual files and information systems are checked for the data in respect of which the access request is made.
5. The Co-ordinator will ensure that the information is supplied promptly and within the time specified by Data Protection legislation and GDPR.
6. Before supplying the information to the individual the Co-ordinator will check each item of data to establish if any of the modifications in respect of health or social work data.
7. If data relating to a third party is involved, it will not be disclosed without the consent of the third party, or the data will be anonymised in order to conceal the identity of the third party.
8. The Co-ordinator will ensure that the information is provided in a form which is clear to the ordinary person.
9. The individual will be informed within the time s specified by Data Protection legislation and GDPR after the request if no information is held on them.

10. School email accounts are the property of the employer and the data controller may need to access individual email accounts if necessary.

9(a) Access Requests by Students: Age of Consent for Access Requests

In relation to access requests made by a student, the Office of the Data Protection Commissioner has recommended that the following guidance be followed as a general rule:

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

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

A student aged from twelve up to and including seventeen can be given access to their personal data, depending on the age of the student and the nature of the record, ie, it is suggested that:

- If the information is ordinary, routine, or non-controversial (eg. a record of a test result) the student could readily be given access.
- If the information is of a sensitive nature, it would be prudent to seek parental/guardian consent in writing before releasing the data to the student. Where the parent/guardian does not give their consent to releasing the data to the student, legal advice should be sought.
- If the information would be likely to be harmful to the individual concerned, parental/guardian consent should be sought before releasing the data to the student.

In the case of students under the age of twelve, an access request may be made by their parent or guardian on the student's behalf. The consent of the child need not be obtained. However, the school must note that the right of access is a right of the data subject themselves (i.e. it is the right of the student). Therefore, access documentation should be sent to the address of the child at his address which is registered with the school as being his home address. It should not be addressed or sent to the parent who made the request. This may present particular difficulties in the case of separated parents.

9(b) Copy to Parents where Students Make Access Request

Where an access request is made by a student under 18 years, the school may choose to have a provision in the School's Data Protection Policy informing the student that:

- Where they make an access request, their parents may be informed that they have done so.
- A complete copy of the access request materials being furnished to the data subject by the school may also be furnished to the student's parent/guardian.

9(c) Parental Access Requests

A parent/guardian may make an access request asking for their child's data. The school must always remember that the right of access is a right of the data subject (i.e., it is the student's right) and therefore the parent/guardian is making the request on behalf of the child. In such a case, the access materials should be sent to the child, not to the parent who requested them. This means that the documentation should be sent to the address at which the child is registered on the school's records and should be addressed to the child. The documentation should not be sent to or addressed to the parent/guardian who made the request. Where parents are separated/estranged, it can be difficult for one parent to accept that they may have less involvement in their child's life. They may feel that they do not have all the information in relation to their child's life in school. Accordingly, the parent may see a section 4 access request as an opportunity to "look into the life of the child". As access materials are sent to the child themselves (not to the parent who made the request) the non-custodial parent may feel frustrated by the lack of information. In such circumstances, the school may invite the parent to make an application under section 11 Guardianship of Infants Act 1964 which 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, the school can release the data on foot of the court order.

9(d) 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 be likely to cause serious harm to his or her physical or mental health. This is to protect the individual from hearing anything about himself or herself which would be likely to cause serious harm to their physical or mental health or emotional well-being. In the case of health data, the information can only be released after the school has consulted with the appropriate health professional (usually the data subject's GP).

Personal Data obtained while carrying on social work ("social work data") (personal data kept for or obtained in the course of carrying out social work by a Government department, local authority, the HSE etc) is also restricted in some circumstances if that would be likely to cause serious harm to the health or emotional condition of the data subject concerned. In the case of social work data, the information cannot be supplied at all if the school believes it would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject. If the social work data includes information supplied to the school by an individual (other than one of the school's employees or agents) while carrying out social work, the school is not permitted to supply that information to the data subject without first consulting that individual who supplied the information.

9(e) Exemptions from a data access request

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

1. Section 5 of the Data Protection Act provides that the right of access does not apply in several 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.

7. If the data subject knows of specific data that the data controller may have omitted as part of a data access request then he/she should notify the data controller within 28 days of receiving his/her data to request the specific data that may have been overlooked.

8. Where the school refuses to hand over some or all 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 will advise the data subject of this in writing, setting out reasons for the refusal, and notifying the data subject that he or she has the right to complain to the Office of the Data Protection Commissioner about the refusal

10. Implementation Arrangements, Roles and Responsibilities

The Principal of Clonkeen College and delegated officers are responsible for implementing this policy. However, all employees who collect and/or control the contents and use of personal data are individually responsible for compliance with the data protection legislation. School personnel should familiarise themselves with this policy and immediately notify the Data Controller (the Board of Management) if they have any concerns.

Personal Data on Enrolment Application Form and Post Enrolment Documentation.

Clonkeen College is registered as a Data Controller under the Data Protection Acts 1988 and 2018 and GDPR. The personal data supplied on this application form and post enrolment documentation is required for the purposes of student enrolment, registration, administration, child welfare and to fulfil our other legal obligations. Contact details will also be used to notify you of school events or activities. While the information provided will generally be treated as confidential to Clonkeen College, from time to time it may be necessary for us to exchange personal data on a confidential basis, where we are legally required to do so, with other bodies including the Department of Education & Skills, the Department of Social & Family Affairs, An Garda Síochána, the Health Service Executive, the National Educational Welfare Board or with another school (where the student is transferring). We may also exchange enrolment information as specified in section 66(6) of the Education (Admission to Schools) Act 2018 which allows for the sharing of certain information between schools to facilitate the efficient admission of students. We rely on parents/guardians to provide us with accurate and complete information and to update us in relation to any change in the information provided. Should you wish to update or access your/your child's personal data you should write to the school Principal, Clonkeen College.

Photographs of Students

The school maintains a database of photographs of school events held over the years. It has become customary to take photos of students engaged in activities and events in the interest of creating a pictorial as well as historical record of life at the school. Staff are permitted to take digital/video images to support educational aims but must follow school policies concerning the distribution of those images, which should only be taken on school equipment. Photographs may be published on the school website, Twitter accounts, school electronic communication systems, in brochures, in newsletters, in local and national newspapers and similar school-related productions. In the case of website photographs, student names will not be recorded with the picture. If you or your child are not happy to have a photograph taken and/or wish to have his photograph removed from the school website at any time you should write to the school Principal.