



Scoil Náisiúnta Droichead An Chláir

Clarecastle National School, Clarecastle, Co. Clare

Reviewed by BOM
November 2020

Data Protection Policy

Ratified by BOM 2015

Clarecastle National School



Data Protection Policy

- 065 682 8274
- school.secretary@clarecastlens.com
- Clarecastle, Co. Clare, V95 T253
- www.clarecastleschool.com

Principal Martin Moloney
Roll Number 17026M

Data Protection Policy

Data Protection Policy of Clarecastle National School

Introductory Statement

The school's Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 and 2003.

The 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. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

Data Protection Principles

The school is a *data controller* of *personal data* relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the school is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 which can be summarised as follows:

Obtain and process *Personal Data* fairly:

Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians 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 and the terms of this Data Protection Policy. The information will be obtained and processed fairly.

Keep it only for one or more specified and explicit lawful purposes:

The School will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.

Process it only in ways compatible with the purposes for which it was given initially:

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

Keep *Personal Data* safe and secure:

Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the 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.

Keep Personal Data accurate, complete and up-to-date:

Parents/guardians, 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. It is the sole responsibility of the parent/guardian, and/or staff member to ensure the school is supplied with accurate and up to date information. 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.

Ensure that it is adequate, relevant and not excessive:

Only the necessary amount of information required to provide an adequate service will be gathered and stored.

Retain it no longer than is necessary for the specified purpose or purposes for which it was given:

As a general rule, the information will be kept for the duration of the individual's time in the 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.

Provide a copy of their *personal data* to any individual, on request:

Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

Purpose of the Policy:

The Data Protection Acts 1988 and 2003 apply to the keeping and processing of *Personal Data*, both in manual and electronic form. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, students and their parents/guardians how their data will be treated.

The 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 school handles or processes their *Personal Data* in the course of their dealings with the school.

Definition of Data Protection Terms

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

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

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

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

Data Controller for the purpose of this policy the Data Controller is the Board of Management, Clarecastle National School.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, the school has a legal responsibility to comply with the Data Protection Acts, 1988 and 2003.

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 more and more data is 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 individual's 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. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and board of management.

Other Legal Obligations

Implementation of this policy takes into account the school's other legal obligations and responsibilities. Some of these are directly relevant to data protection. **For example:**

- 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 their education.
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School
- 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

- 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.
- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a “relevant purpose” (which includes recording a person’s educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)
- 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
- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be “personal data” as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body
- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection
- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & 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).

Relationship to characteristic spirit of the School

In Clarecastle National School we seek to:

- enable each student to develop their full potential
- provide a safe and secure environment for learning
- promote respect for the diversity of values, beliefs, traditions, languages and ways of life in society.

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and others who interact with us.

The school wishes to achieve these aims/missions while fully respecting individuals’ rights to privacy and rights under the Data Protection Acts.

Personal Data

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

- 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.

(c) Location:

Data will be stored in both automated and manual form in a manner in which 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. Any breach of confidentiality will lead to disciplinary action being initiated by the Board of Management under agreed procedures.

(d) Security:

Manual records (personal file within a *relevant filing system*) will be retained in a locked filing cabinet in the Principal's Office. The office will be locked when not occupied. A coded lock provides additional security to the door of the Principal's Office. During

prolonged absences from the office the door adjoining the secretary's office will be locked. The secretary's office will be locked using a coded lock during prolonged absences of the secretary during the working day.

Automated Records will be retained on hardware that is password protected. Each system (OLCS, Aladdin) will require a username and password to be input. Passwords will be changed at regular intervals. The office will be locked when not occupied. A coded lock provides additional security to the door of the Principal's Office. During prolonged absences from the office the door adjoining the secretary's office will be locked. The secretary's office will be locked using a coded lock during prolonged absences of the secretary during the working day.

B. *Student records:*

(a) **Categories of student data:** These may include:

The following information may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school.

*In line with the provisions of Department of Education & Skills Primary Circular 0017/2014 it is **MANDATORY** that all pupils enrolled in Clarecastle National School have the following information uploaded on the Primary Online Database (POD). For further details in relation to **POD** please refer to **Primary Circular 0025/2015** and **POD Fair Processing Notice** appended to this document.*

Information recorded will include:

Category 1 Information: Sought on Enrolment Application Form.

- Forename of pupil
- Surname of pupil
- Birth Certificate Forename (*if different from above*)
- Birth Certificate Surname (*if different from above*)
- PPSN
- Mother's Maiden Name
- Date of Birth
- Gender
- Address
- County of Residence
- Nationality

Other Category 1 Information:

- Class
- Standard
- Enrolment Date
- Leaving Indicator, Date & Destination
- Pupil Retained Indicator
- Pupil Integrated Indicator
- Indicator for receipt of Learning Support

- Indicator of Pupil SEN assessment
- Pupil Special Class Type
- Pupil SEN Type
- Mother Tongue
- Year of arrival in Ireland
- Pupil Deceased Indicator
- DPIN (Department Pupil Identifier)

Category 2 Information: Sensitive personal data for which Parental Consent will be sought before uploading the following on POD.

- Ethnicity/Cultural Background
- Pupil Religion

Other information which may be requested/retained by the school for pupils enrolled:

- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student)
- Psychological, psychiatric and/or medical assessments
- Attendance records
- Photographs and recorded images of students (including at school events and noting achievements).
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. records of any serious injuries/accidents etc.
- Communication from Parents/Guardians
- 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).

(b) Purposes:

The purposes for keeping student records are:

- to enable each student to develop to their full potential
- to validate pupil identity on Department of Education and Skills Primary Online Database (POD).
- 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/guardians 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 celebrate school achievements, compile yearbooks, maintain the school website, record school events, and to keep a record of the history of the school.
 - 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 National Council for Special Education, TUSLA, and other Schools etc. in compliance with law and directions issued by government departments
 - to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information held.
- (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. Any breach of confidentiality will lead to disciplinary action being initiated by the Board of Management under agreed procedures.
- (d) **Security:**

Manual records (personal file within a *relevant filing system*) will be retained in a locked filing cabinet in the "Strong Room" which is located off the main entrance hallway. The room is fitted with a metal door and has a double locking system. The keys to access the room are held in the locked keybox in the secretary's office. The secretary's office will be locked using a coded lock during prolonged absences of the secretary during the working day.

Automated Records will be retained on hardware that is password protected. Each teacher will use a specific user name and password to access the pupil database Aladdin. Teachers will only have access to the details/records of pupils for whom they have direct responsibility. Passwords will be changed periodically by the system administrator, normally the Principal, Martin Moloney.

Deputy Principal, Teresa Nugent has special access to information pertaining to attendance in her role as Attendance Officer.

Post Holder Carmel Nugent has special access to information in relation to testing.

Passwords for hardware and software must not be left accessible.

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) Purposes:

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.

- (c) Location:** In a secure, locked filing cabinet and that only personnel who are authorised to use the data can access it. Employees are required to maintain the confidentiality of any data to which they have access. Any breach of confidentiality will lead to disciplinary action being initiated by the Board of Management under agreed procedures.

(d) Security:

Manual records (personal file within a *relevant filing system*) will be retained in a locked filing cabinet in the Principal's Office. The office will be locked when not occupied. A coded lock provides additional security to the door of the Principal's Office. During prolonged absences from the office the door adjoining the secretary's office will be locked. The secretary's office will be locked using a coded lock during prolonged absences of the secretary during the working day.

Automated Records will be retained on hardware that is password protected in the Principal's Office. The office will be locked when not occupied. A coded lock provides additional security to the door of the Principal's Office. During prolonged absences from the office the door adjoining the secretary's office will be locked. The secretary's office will be locked using a coded lock during prolonged absences of the secretary during the working day.

D. 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 cabinet in the administration 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. Any breach of confidentiality will lead to disciplinary action being initiated by the Board of Management under agreed procedures.

(d) Security:

Manual records (personal file within a *relevant filing system*) will be retained in a locked cabinet in the Administration Office. The administration office will be locked using a coded lock during prolonged absences of the relevant personnel during the working day.

Automated Records will be retained on hardware that is password protected in both the Administration Office & The Principal's Office. The office will be locked when not occupied. A coded lock provides additional security to the door of the Principal's Office. During prolonged absences from the office the door adjoining the secretary's office will be locked. The secretary's office will be locked using a coded lock during prolonged absences of the secretary during the working day.

CCTV images/recordings

- (a) **Categories:** CCTV is installed in our school. Cameras are located externally to cover perimeter walls/fencing and internally, in the reception lobby area. 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 in the reception lobby area. CCTV recording equipment is located in the administration office of school.
- (d) **Security:** Access to images/recordings is restricted to the Principal, Martin Moloney and Deputy Principal, Teresa Nugent, or, in the event of their absence the person designated to act on their behalf. Hard disk recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

Links to other school policies and curriculum delivery:

Our school policies need to be consistent with one another, within the framework of the overall Plean Scoile. 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 may be among those considered:

- Child Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Personal Internet Enabled Device Policy
- Admissions/Enrolment Policy
- CCTV Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE/RSE etc.

Processing in line with data subject's rights

Data in this school will be processed in line with the data subjects' rights.

Data subjects have a right to:

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

Dealing with a data access requests

Section 3 access request

Under Section 3 of the Data Protection Acts, 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 and the data controller will **accede to the request within 21 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.
- 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 40 days
- Fee may apply but cannot exceed €6.35
- 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 our school, 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.
- Request the caller to supply a landline/office number that the staff member can contact them on by return call.
- Refer the request to the Principal/Deputy Principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Implementation arrangements, roles and responsibilities

In our school the Board of Management is the data controller. The Principal, or in his absence the Deputy Principal, is assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

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

Name	Responsibility
Board of Management:	Data Controller
Principal: Mr. Martin Moloney	Implementation of Policy
Deputy Principal: Mr. MJ Malone	Implementation of Policy
Teaching personnel:	Awareness of responsibilities & confidentiality.
Special Needs Assistants:	Awareness of responsibilities & confidentiality.
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

Covid-19

In dealing with issues in relation to Covid-19 the Board of Management and relevant staff members must ensure compliance with GDPR protocols.

- The school will not inform anyone other than the parents if a student is sent home due to his/her symptoms.
- The principal may be obliged to inform relevant staff on a need to know basis in order to manage a given situation.
- All families are entitled to confidentiality. The school cannot identify individuals to the school community.
- Staff should be familiar with the protocols and of their data protection responsibilities.
- Current Public Health legislation empowers the HSE to request specific information in relation to pupils from the school. A parent cannot withdraw consent to a school from forwarding a pupil's personal data to the HSE.

Remote Learning

When engaged in remote learning and exchanging information electronically all staff will adhere to the principles of GDPR.

Ratification & communication

This Policy will be made available to the school community. The Policy was ratified by the Board of Management of Clarecastle National School at a meeting held on the 09/11/2020.

Monitoring the implementation of the policy

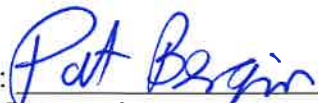
The implementation of the policy shall be monitored by the Principal and Board of Management.

An annual report will be issued to the Board of Management to confirm that the actions/measures set down under the policy are being implemented.

Reviewing and evaluating the policy

The policy will be reviewed and evaluated at certain pre-determined times and as necessary. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or the NEWB), legislation and feedback from parents/guardians, 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.

Signed:


Pat Bergin
Chairperson BOM

Date: 09/11/2020

Records Retention Schedule

Retention of Records

The following record retention schedule clarifies the length of time for which personal data will be kept and the reasons why the information is being retained.

In determining appropriate retention periods, the Board of Management have had due regard for statutory obligations imposed on it as data controller.

If the purpose for which information obtained has ceased and the personal information is no longer required, the data will be deleted or disposed of in a secure manner. Data may also be anonymised to remove any personal data. Anonymisation will be irrevocable.

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

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

WARNING: In general, the limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim and the Statute of Limitations may be different in every case. In all cases where reference is made to "18 years" being the date upon which the relevant period set out in the Statute of Limitations commences for the purposes of litigation, the school is aware that in some situations (such as the case of a student with special educational needs, or where the claim relates to child sexual abuse, or where the student has not become aware of the damage which they have suffered, and in some other circumstances), the Statute of Limitations may not begin to run when the student reaches 18 years of age and specific legal advice will be sought by schools on a case-by-case basis. In all cases where retention periods have been recommended with reference to the relevant statutory period in which an individual can make a claim, these time-frames may not apply where there has been misrepresentation, deception or fraud on the part of the respondent/defendant. In such a circumstance, the school is aware that a claim could arise many years after the incident complained of and the courts/tribunals/employment fora may not consider the complainant to be "out of time" to make their claim.

Clár Leabhar/Rolla

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

Pupil Records

Records relating to pupils/students	Primary	Confidential shredding	Comments
Enrolment Forms	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Student transfer forms (Applies from primary to primary; from one second-level school to another)	If a form is used- Student reaching 18 years + 7 years	Confidential shredding	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Disciplinary notes	Never destroy	N/A	Never destroy
Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results)	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school).
End of term/year reports	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Records of school tours/trips, including permission slips, itinerary reports	Never destroy	N/A	Never destroy
Scholarship applications e.g. Gaeltacht, book rental scheme	Student reaching 18 years + 7 years	Confidential shredding	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for

			proceedings to be served on the school)
Garda vetting form & outcome - STUDENTS	N/A as primary school pupils will not be undergoing vetting	Confidential shredding	Record of outcome retained for 12 months. School to retain the reference number and date of disclosure on file, which can be checked with An Garda Siochana in the future.

Sensitive Pupil Data

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

			name, parent not being contacted to be informed of parent-teacher meeting) or other minor matter, then student reaching 18 years + 7 years (6 years in which to take a claim, and 1 year for proceedings to be served on school)
--	--	--	--

Staff Records Recruitment	Primary	Final disposition	Comments
Recruitment process Note: these suggested retention periods apply to unsuccessful candidates only. They do NOT apply to successful candidates, or candidates who are/were also employees already within your school applying for another post/position. For successful candidates, or candidates who are/were also employees already within your school applying for another post/position, see retention periods set out below.	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Applications & CVs of candidates called for interview	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Database of applications	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Selection criteria	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.

Applications of candidates not shortlisted	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Unsolicited applications for jobs	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Candidates shortlisted but unsuccessful at interview	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Candidates shortlisted and are successful but do not accept offer	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Interview board marking scheme & board notes	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Panel recommendation by interview board	✓	Confidential shredding	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.
Correspondence from candidates re feedback	✓	N/A	Depends upon nature of feedback. If feedback is from unsuccessful candidate who is not an employee within the school, keep in line with retention periods in "Staff Records" above. If

			<p>feedback is from successful candidate or from unsuccessful candidate who is already an employee within the school, keep in line with “Staff personnel while in employment”.</p>
--	--	--	--

Staff Files

Staff personnel files (whilst in employment)	Primary	Final Disposition	Comments
e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, records of staff training etc.		Confidential shredding. Retain an anonymised sample for archival purposes.	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Application &/CV	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Qualifications	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
References	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Interview: database of applications (the section which relates to the employee only)	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Selection criteria	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the

			school, plus 1 year for proceedings to be served on the school)
Interview board marking scheme & board notes	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Panel recommendation by interview board	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Recruitment medical	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Job specification/description	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Contract/Conditions of employment	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Probation letters/forms	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for

			proceedings to be served on the school)
POR applications and correspondence (whether successful or not)	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Leave of absence applications		Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Job share	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Career Break	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Maternity leave	✓	Confidential shredding	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)
Paternity leave	✓	Confidential shredding	Retain for 2 years following retirement/resignation or the duration of employment plus 7 years (6 years in which to take

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

			requirement to retain for 3 years
Allegations/complaints	✓	Doesn't have a time period advised	Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). Please note the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.
Grievance and Disciplinary records	✓		Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). Please note the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.

Medmark/Occupational Health

Occupational Health Records	Primary	Confidential Shredding	Comments
Sickness absence records/certificates	✓	Confidential shredding Or do not destroy.	Re sick leave scheme (1 in 4 rule) ref DES C/L 0060/2010 Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.

Pre-employment medical assessment	✓	Confidential shredding Or do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Occupational health referral	✓	Confidential shredding Or Do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Correspondence re retirement on ill-health grounds	✓	Confidential shredding Or Do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Accident/injury at work reports	✓	Confidential shredding	Retain for 10 years, or the duration of the employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), whichever is the greater (unless sickness absence relates to an accident/ injury/ incident sustained in

			relation to or in connection with the individual's duties within the school, in which case, do not destroy).
Medical assessments or referrals	✓	Confidential shredding Or Do not destroy.	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless Medmark assessment relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.
Sick leave records (sick benefit forms)	✓	Confidential shredding	In case of audit/refunds, Current year plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)

Payroll

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

Pension increases (notification to Co.)	✓	Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)
Salary claim forms	✓	Confidential shredding	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)

Board of Management

Board of Management Records	Primary	Final disposition	Comments
Board agenda and minutes	✓	N/A	Indefinitely. These should be stored securely on school property
School closure	✓		On school closure, records should be transferred as per Records Retention in the event of school closure/amalgamation . A decommissioning exercise should take place with respect to archiving and recording data.
Other school based reports/minutes	Primary	Final disposition	Comments
CCTV recordings	✓	Safe/secure deletion.	28 days in the normal course, but longer on a case-by-case basis e.g. where

			recordings/images are requested by An Garda Síochána as part of an investigation or where the records /images capture issues such as damage/vandalism to school property and where the images/recordings are retained to investigate those issues.
Principal's report to Board of Management	✓	N/A	Indefinitely. Administrative log and does not relate to any one employee in particular: the monthly reports are not structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Not a "relevant filing system".
Finance			
Financial Records	Primary	Final disposition	Comments
Audited Accounts	✓	n/a	Indefinitely
Payroll and taxation	✓		Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system.
Invoices/back-up records/receipts	✓	✓	Retain for 7 years

In School Management

Promotion process	Primary	Final Disposition	Comments
Posts of Responsibility	✓	N/A	Retain indefinitely on master file as it relates to pay/pension etc. (See DES guidelines)
Calculation of service	✓	N/A	Retain indefinitely on master file
Promotions/POR Board master files	✓	N/A	Retain indefinitely on master file
Promotions/POR Boards assessment report files	✓	N/A	Retain original on personnel file in line with retention periods in "Staff Records" retention guidelines above
POR appeal documents	✓	N/A	Retain original on personnel file, and copy of master & appeal file. Retain for duration of employment + 7 years (6 years in which to take a claim, plus 1 year to serve proceedings on school). Copy on master and appeal file.

Clarecastle National School

Data Access Procedures

The Data Protection Acts, 1988 and 2003 provide for a right of access by an individual data subject to personal information held by Clarecastle National School. The following procedure is provided to ensure compliance with Clarecastle National School's obligations under the Acts and governs the manner in which requests for access to personal data will be managed by the school authorities.

A data subject would be required to familiarize themselves with the procedure and to complete the Data Access Request Form which will assist the school in processing the access request where personal information (or in the case of a parent/guardian making an access request on behalf of a student, personal information in relation to their child) as a data subject is processed and retained by the school.

It is important to note that only personal information relating to the individual (or in the case of a parent/guardian making an access request on behalf of a student, only personal information in relation to his/her/their child) will be supplied. No information will be supplied that relates to another individual.

Important note to students making access requests:

Where a student (aged under 18 years) makes an access request, the school may inform the student that:

- (a) Where they make an access request, their parents 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/guardian.

This is provided for in the school's Data Protection Policy. The right of access under the Data Protection Acts is the right of the data subject. However, there may be some data held by the school which may be of a sensitive nature and the school will have regard to the following guidance issued by the Office of the Data Protection Commissioner in relation to releasing such data:

- A student aged eighteen years or older (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.
- If a student aged eighteen years or older has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.
- 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, i.e. it is suggested that:
 - If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
 - If the information is of a sensitive nature, it would be prudent to seek parental/guardian consent before releasing the data to the student

- 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. 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 addressed to the child at his/her address which is registered with the school as being his/her home address. It should not be addressed or sent to the parent who made the request.

For further information, see "Important Note to Parents Making Access Requests on Behalf of their Child" below.

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

Where a parent/guardian makes an access request on behalf of their child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the 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/guardian who made the request.

Where a parent/guardian is unhappy with this arrangement, the parent/guardian 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/guardian, a copy of the order should be given to the school by the parent/guardian and the school can release the data on foot of the court order.

Individuals making an access request

On making an access request, any individual (subject to the restrictions in Notes A and B below) about whom a 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 his/her 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 program 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.

Data access requirements

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

1. Apply in writing requesting access to your data under section 4 Data Protection Acts or, alternatively, request an Access Request Form which will greatly assist the school in processing your access request more quickly.

All correspondence should be addressed to:

The Chairperson,
Board of Management,
Clarecastle National School,
Clarecastle,
Co. Clare.

2. You will be provided with a form which will assist the school in locating all relevant information that is held subject to the exceptions and prohibitions outlined in **Appendix A**. 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.

3. On receipt of the 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 Clarecastle National School the co-ordinator is:
The Chairperson of the Board of Management

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.

4. 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.
5. 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.
6. The co-ordinator will ensure that the information is supplied promptly and within the advised timeframes in items 7, 8 and 9 as appropriate.
7. **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/guardian of a student aged under 18 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/her 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 21 days of receipt of the access request form and no fee will apply.**
8. **Where a request is made under Section 4 of the Data Protection Acts**, the following information will be supplied within **40 days and an administration fee of €6.35 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/her (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/her 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 program 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.
9. Where a request is made with respect to **examination results** an increased time limit of **60 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.
 10. Before supplying the information requested to you as data subject (or where the access request is made on behalf of a student aged under 18 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.
 11. 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.

12. Where a school may be unsure as to what information to disclose, the school reserves the right to seek legal advice.
13. The co-ordinator will ensure that the information is provided in an intelligible form.
14. Number the documents supplied.
15. A response will be "signed-off" by The Chairperson of the Board.
16. The school will respond to your access request within the advised timeframes contingent on the type of request made.
17. The school reserves the right to supply personal information to an individual in an electronic format e.g. on tape, USB, CD etc.
18. 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.
19. Where you as an individual data subject may seek to rectify incorrect information maintained by the school, please notify the school and a form will be supplied to you for this purpose. 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.
20. In circumstances where your access request is refused, *Clarecastle National School* 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.
21. **Where requests are made for CCTV footage**, an application must be made in writing and the timeframe for response is within 40 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, disk, USB, with relevant images. 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.

There are a number of exceptions to the general rule of right of access, including those specified in Notes A and B in **Appendix A**.

This procedure is regularly reviewed in line with the Clarecastle National School's commitment to its responsibilities under Data Protection Legislation.

Appendix A

Note A: Access requests by students

- A student aged **eighteen years or older** (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.
- If a student aged **eighteen years or older** has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.
- 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, i.e. it is suggested that:
 1. If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access.
 2. 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
 3. 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 addressed to the child at his/her address which is registered with the school as being his/her home address. **It should not be addressed or sent to the parent who made the request.** For further information, see "Important Note to Parents Making Access Requests on Behalf of their Child" below.
- In any of the circumstances outlined above, if the data contains health data and disclosure would be likely to cause serious harm to the physical or mental health of the individual concerned, the school is obliged to withhold the data until they have consulted with the data subject's medical practitioner and (in the case of a student under 18 or a student with special educational needs whose disability or medical condition would impair his or her ability to understand the information), parental/guardian consent should also be sought.
- In some cases (i.e. where the information is "**health data**"), it is advised that the data be supplied by the medical practitioner.
- In any of the circumstances outlined above, if the data contains **social work data** and disclosure would be likely to cause serious harm to the physical or mental health of the individual, the school is not permitted to release the data to the individual.

Note B: Exceptions to note:

Data protection regulations prohibit the supply of:

1. 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).

2. *Personal Data* obtained in the course of 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/ETB'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.

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 (like 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 or she has the right to complain to the Office of the Data Protection Commissioner about the refusal.

CLARECASTLE NATIONAL SCHOOL

Data Access Request Form

Date issued to data subject: DD/MM/YYYY

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

Important: Proof of Identity must accompany this Access Request Form (eg. official/State photographic identity document such as driver's licence, passport).

A fee of €6.35 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/Guardian 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 <Name of School> 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 <Name of School> 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 €6.35 ☐

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/ETB 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 <name of school> in the amount of €6.35 where a Section 4 request is made? (Please do not send us €6.35 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:

Once satisfied as to the identity of the individual a note will be made in school records that suitable identification provided, the school will not retain a copy of the identity document.

Please return this form to:

Chairperson of Board of Management

Clarecastle National School

Protocol for use of Laptops and Other Mobile Storage Devices (incl. Mobile Phones, PDAs, USB memory sticks, External Hard Drives, etc.)

Laptops and Other Mobile Storage Devices (incl. Mobile Phones, PDAs, USB memory sticks, External Hard Drives, etc.) are useful tools to meet the professional needs of staff. They are, however, highly susceptible to loss or theft. To protect the content held on these devices, the following recommendations must be followed by all staff members using school equipment:

1. All staff members using Board of Management Laptops must sign a Laptop Use Agreement
2. All portable devices will be password protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, both a Username and login password be used. Passwords used on these devices should be of sufficient strength to deter password cracking or guessing attacks.
3. A password will be randomly generated alpha numeric.
4. Personal, private, sensitive or confidential data should not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be encrypted. With regard to laptops, full-disk encryption must be employed, regardless of the type of data stored
5. Data held on portable devices will be backed up daily at a scheduled time of 1.00pm to the school server.
6. When portable computing devices are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons
7. Portable devices must not contain unauthorised, unlicensed or personally licensed software. All software must be authorised and procured through the school authorities.
8. Anti-virus/anti-spyware/personal firewall software is installed and kept up-to-date on portable devices. These devices are subjected to regular virus checks using this software
9. Departments should ensure that when providing portable devices for use by staff members, each device is authorised for use by a specific named individual. The responsibility for the physical safeguarding of the device will then rest with that individual
10. Portable devices should never be left in an unattended vehicle
11. Staff owned devices such as portable media players (e.g. iPods, etc.), digital cameras, USB sticks, etc. are technologically restricted from connecting to Department computers
12. Departments should implement procedures that will ensure that personal data held on mobile storage devices is fully deleted when the data is no longer required (e.g. through fully formatting the device's hard drive).

