



Cork Educate Together Secondary School

Data Protection Policy 1.0 June 2017

SECTION A

1. Introduction

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.

The School has the following security measures in place to ensure that all access to data is appropriate and relevant:

- All computers have a password log-on.
- Networked computer screens have a password enabled screensaver.
- Student and teachers have access to different network shares and to their own areas which are password protected
- School staff and students are on the Exchange domain but have different levels of access privileges. This is standard protocol and procedure for virtualised servers and cloud provision.
- All personal files are kept in a locked filing cabinet or in a lockable office in line with Clean Desk Policy
- Staff members are responsible for all data that they take off site, either in a digital format or otherwise. They should also maintain their security status by both protecting their passwords and changing them frequently.
- All data security breaches must be reported immediately to the Principal.
- The Principal and Deputy have an added responsibility for student/family data as they hold access to all parent and student passwords (VSWare, Schoology).
- All student files are kept in a locked filing cabinet or in a lockable office in line with Clean Desk Policy

- Information on computer screens and manual files are kept out of view of callers to the school. Staff should press the 'Control + Alt+ Delete' keys to lock a screen when they are finished using a computer.
- In line with the Clean Desk policy, no personal details of staff, students or parents/guardians are to be left on desks overnight.
- All requests for data must include the reason for which the data is being collected.
- No details may be forwarded to any third party without the express permission of the parties concerned.
- Data related to students who decline a place are shredded immediately, once notification is received
- Data associated with visitors to the school are shredded at the end of each year
- Access to data is restricted to authorised staff (Principal, Deputy Principal, HR Operations Manager)

2. Scope

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.

3. Relationship to characteristic spirit of the School

CETSS offers parents the choice of an education based on the inclusive intercultural values of respect for difference and justice and equality for all. In our school, every child will learn in an inclusive, democratic, co-educational setting that is committed to enabling and supporting each child to achieve their full potential while at the same time preparing them to become caring and active members of a culturally diverse society.

Adapted from Educate Together Mission Statement

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

4. Definition of Terms

Data: means information in a form which can be processed. It includes automated data (information on computer or information recorded with the intention of putting it on computer) and manual data (information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system).

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

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

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 is the Board of Management, CETSS.

VSWare: The school's admin system (timetabling, reports generation, behaviour monitoring etc.)

Post Primary Online Database (PPOD): The Department of Education's database, through which most school funding and staffing is determined.

Educational Progress: According to the JMB, the term **Educational Progress** must be defined in individual school's Data Protection Policy. This refers to the particular information, to which parents/legal guardians are entitled as pertaining to their child's education.

We define these entitlements as being limited to the following:

- consultation regarding the educational welfare of child,
- notice of formal parent teacher meetings,
- copies of school reports,
- notice of meetings with NEPS, SENO etc.
- notice of in-school/after school programmes,
- notice of school closures,

This definition has implications for parental access to online platforms. This technology can potentially grant parents greater and more consistent access to information. In accordance with the above criteria, we shall therefore facilitate parental/guardian access to:

1. *VSWare*- parents/legal guardians can view reports, behavioural incidents, and attendance records.
2. *Schoology*- parents/legal guardians can view grades for homework, participation, and projects, as well as the resources given to the students by teachers. However,

individual student's homework submissions are considered to be their personal data and can only be accessed through them, with their consent.

5. 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.

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/guardians of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in his or her education.
- 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, the 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).

6. Policy Objectives

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

SECTION B: 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.)
- Records of salary grade
- Records of teaching registration
- Records of Garda vetting
- Records of staff contracts
- Bank account details
- 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).

Note: a record of grievances may be maintained which is distinct from and separate to individual personnel files.

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

(d) **Security:** Records are primarily kept as manual records in a *relevant filing system*, though are also occasionally stored as computer records also (databases such as PPOD and VSWare). Manual copies are kept under lock, whilst digital content is password protected.

CVs sent in by people seeking employment will be stored securely by the secretary and or management and kept for a number of years as candidates could be potential sources of substitution for absent teachers. After a reasonable period of time has elapsed they will be safely disposed of by the holders of the data.

B. Student records:

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

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
 - name, address and contact details, PPS number
 - date and place of birth
 - names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
 - racial or ethnic origin
 - membership of the Traveller community, where relevant
 - whether they (or their parents) are medical card holders
 - whether English is the student's first language and/or whether the student requires English language support
 - any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student
- Psychological, psychiatric and/or medical assessments
- Attendance records
- Photographs and recorded images of students (including at school events and noting achievements). See the template "Guidance on Taking and Using Images of Children in Schools"
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is repeating the Leaving Certificate
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed

- Garda vetting outcome record (where the student is engaged in work experience organised with or through the school which requires that they be Garda vetted)
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the 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).
- Student records will be held by the school for a period of 7 years after their departure.
- N.B. Counsellor data (notes on student/family situations etc.) will be held by the counsellor in a disguised and non-identifiable manner in a secure location by the counsellor: these will be kept for a period of 7 years and then will be safely disposed of. In case of a request from an outside supportive agency (pieta house, Tusla, social workers, etc.) an agreement will be reached between the councillor and parents regarding the release of data.
- N.B. Guidance data (standardised testing) will be kept in a secure place for the duration of their schooling and then safely disposed of. Anonymised versions of this data will be provided to staff for policy development (SSE etc.).
- SEN data (psychologist and medical reports, etc.) will be securely stored by the coordinator for the duration of the students' schooling and then safely disposed of. Summarised versions of this data may need to be occasionally given to the teachers of certain students for the purpose of supporting their educational progress.

(b) **Purposes:** The purposes for keeping student records are:

- to enable each student to develop to their 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 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, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used only with parental permission
- 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/ references to third-level educational institutions and/or prospective employers
 - In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the School will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** Manual records are kept in a locked *relevant filing system*, whilst computer records are kept on VSWare and PPOD and are password protected.

Note: email and log-in data given to students by the school are considered the personal data of the student. The school will not provide this data to any other parties.

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.

- (d) **Security:** Manual records of BOM minutes and Agreed Reports are stored in a locked *relevant filing system*, whilst computer versions are stored in a password protected cloud storage area (One Drive), which is only accessible by the Principal and Secretary.

D. Volunteer records:

Categories of volunteer data: This may include:

- Name, address and contact details
- Records of Garda vetting

(a) **Purposes:** Volunteer records are kept for the purposes of:

- the management and administration of school business (now and in the future)
- 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

(b) **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.

(c) **Security:** Records are primarily kept as manual records in a *relevant filing system*, though are also occasionally stored as computer records also (databases such as PPOD and VSWare). Manual copies are kept under lock, whilst digital content is password protected.

E. Other records:

Creditors

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

- name
- address
- contact details
- PPS number
- tax details
- bank details and

- amount paid.
- (b) **Purposes:** This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** Manual records are maintained in a locked *relevant filing system*), accessible to the Principal and Secretary only.

Charity tax-back forms

- (a) **Categories of data:** the school may hold the following data in relation to donors who have made charitable donations to the school:
- name
 - address
 - telephone number
 - PPS number
 - tax rate
 - signature and
 - the gross amount of the donation.
- (b) **Purposes:** Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the case of audit by the Revenue Commissioners.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** Manual records are maintained in a *relevant filing system*), whilst computer records may be held on VSWare and are password protected.

CCTV images/recordings (Future)

- (a) **Categories:** If and when CCTV is installed, externally i.e. perimeter walls/fencing and internally, these 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 can be located externally and internally as detailed in the CCTV Policy. Recording equipment is located in the Principal's office or in the reception office of school.
- (d) **Security:** Access to images/recordings is restricted to the Principal & Deputy Principal of the school. Tapes, DVDs, 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.

Examination results

- (a) **Categories:** The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual, continuous assessment and mock-examinations results.
- (b) **Purposes:** The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

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.

- (c) **Security:** Manual records of school reports are maintained in a locked *relevant filing system*), whilst results are also maintained digitally on a. VSWare and b. Schoology. This data is shall be available to parents/guardians, so as to enable them to be able to monitor the educational progress of their child.

October Returns

- (a) **Categories:** At the beginning of each academic year (and for 1st year or transferring students, on enrolment) parents/guardians and students are asked to provide the school with certain information so that the School can make returns to the Department of Education and Skills ("DES") referred to as "October Returns". These October Returns will include sensitive personal data regarding personal circumstances which are provided by parents/guardians and students on the basis of explicit and informed consent. The October Return contains individualised data (such as an

individual student's PPS number) which acts as an "identifier" for the DES to validate the data that belongs to a recognised student. The DES also transfers some of this data to other government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection pursuant to the Social Welfare Acts, transfers to the State Examinations Commission, transfers to the Educational Research Centre, and transfers to the Central Statistics Office pursuant to the Statistics Acts. The data will also be used by the DES for statistical, policy-making and research purposes. However the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes. The DES has a data protection policy which can be viewed on its website (www.education.ie). The DES has also published a "Fair Processing Notice" to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (search for Circular Letter 0047/2010 in the "Circulars" section).

- (b) **Purposes:** The school asks parents/guardians and students to complete October Returns for the purposes of complying with DES requirements to determine staffing and resource allocations and to facilitate the orderly running of the school. The main purpose of the October Returns is for the DES to determine whether the student qualifies for English language support and/or additional resources and support to meet their particular educational needs. The October Returns are submitted to the DES electronically. The DES has their own policy governing the security of the data sent to them by all post-primary schools. The co-operation of each student and/or their parents/guardians in completing the October Return is greatly appreciated as the school's aim is to ensure that each student is assisted in every way to ensure that s/he meets his/her full potential.
- (c) **Location:** In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- (d) **Security:** Manual records are maintained in a locked *relevant filing system*, whilst digital records are maintained on two password protected databases, with restricted access: VSWare and PPOD.

SECTION C

The School has arrangements in place to ensure that all personal data records held by the school are obtained, processed, used and retained in accordance with the following eight rules of data protection (based on the Data Protection Acts):

1. Obtain and process information fairly.
2. Keep it only for one or more specified, explicit and lawful purposes.
3. Use and disclose it only in ways compatible with these purposes.
4. Keep it safe and secure.
5. Keep it accurate, complete and up-to-date.

6. Ensure that it is adequate, relevant and not excessive.
7. Retain it for no longer than is necessary for the purpose or purposes.
8. Give a copy of his/her personal data to that individual on written request and photo id.
(Please see attached Appendix)

Minimum Age

The minimum age at which consent can be legitimately obtained for processing and disclosure of personal data under rules 1 and 3 above is not defined in the Data Protection Acts. However, guidance material published on the Data Protection Commissioner’s website states the following:

Minimum age of consent:

“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.”

- Data Protection Commissioner’s website

SECTION D

1. Links to Other Policies

The Child Protection Policy, Guidance Plan, Anti-Bullying Policy, Substance Use Policy and the Code of Behaviour shall, once ratified, be consistent with the Data Protection Policy.

2. Implementation Arrangements, Roles and Responsibilities

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

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

Name	Responsibility
Board of management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality

IT personnel/support:

Security, encryption, confidentiality

3. 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
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

4. Ratification & Communication

This policy has been ratified by the Board of Management and is the school's agreed data protection policy. Staff members are familiar with the policy and it has been circulated within the school community. Staff members will be made aware of any changes in the way the school records information on students, staff and others in the school community. Parents/guardians and students are informed of the data protection policy from the time of enrolment of the student by means of the Statement of Data Protection.

5. Implementation, Monitoring and Review of the Policy

This policy will apply from the 2016/2017 school year and thereafter and will be monitored by school management. The policy will be reviewed early in the 2017/18 academic year.

Appendix 1- Data Protection Statement

(for inclusion on relevant forms when personal information is being requested)

The information collected on this form will be held by The School in manual and in electronic format. The information will be processed in accordance with the Data Protection Act, 1988 and the Data Protection (Amendment) Act, 2003.

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

Disclosure of any of this information to statutory bodies such as the Department of Education and Science or its agencies will take place only in accordance with legislation or regulatory requirements. Explicit consent will be sought from parents/guardians or students aged 18 or over if the school wishes to disclose this information to a third party for any other reason.

Parents/guardians of students and students aged 18 or over have a right to access the personal data held on them by the school and to correct it if necessary.

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

Signed Parent/Guardian: _____

Signed Student: _____

Appendix 2 – Compliance with the Eight Rules of Data Protection

1. Obtain and process information fairly

- Procedures are in place to ensure that staff members, parents/guardians and students are made fully aware when they provide personal information of the identity of the persons who are collecting it, the purpose in collecting the data, the persons or categories of persons to whom the data may be disclosed and any other information which is necessary so that processing may be fair (as stated above, the sample statement in Appendix 1 could be included on relevant forms where personal information is being requested).
- Personal information is processed fairly in accordance with the Data Protection Acts, with consent being obtained from staff members, parents/guardians or students, where required.
- Sensitive personal information is processed fairly in accordance with the Data Protection Acts, with explicit consent being obtained from staff members, parents/guardians or students, where required.

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

- Persons whose data is collected know the reason why it is collected and kept and the purpose for which the data is collected.
- School management is aware of the different sets of data which are kept and the specific purpose of each.

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

- Data is used only in ways consistent with the purpose/s for which it was obtained and is only disclosed in ways consistent with that purpose.
- There is a procedure in place, which is in accordance with the Data Protection Acts facilitates the transfer of information to another school when a student transfers. (Student Transfer Form – See appendix)
- In accordance with legislation (Education Welfare Act 2000, Child Protection Guidelines) personal data will be disclosed to third parties like the Department of Education and Science, the NEWB, Gardaí, in legal proceedings and HSE personnel.
- There is a procedure in place, which is in accordance with the Data Protection Acts facilitate the transfer of personal data abroad.

Exceptions to disclosure rule:

- Data can be disclosed when required by law
- Data can generally be disclosed to an individual himself/herself or with his/her consent.

4. Keep it safe and secure

Security measures are to be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

- Access to the information (including authority to add/amend/delete records) is restricted to authorised staff on a “need to know” basis.
- The Administration Manager, Principal, Deputy Principal has access to what information is based on this “need to know” policy.
- Computer systems are password protected.
- Information on computer screens and manual files are kept out of view of callers to the school/office.
- Back-up procedures are in operation for computer held data, including off-site back-up.
- All reasonable measures are taken to ensure that staff are made aware of security measures and comply with them.
- All waste papers, printouts etc. are disposed of carefully.
- All steps are taken to ensure that no unauthorised person can access data from computers which are no longer in use or subject to change of use.
- There is a designated person responsible for security.
- There are periodic reviews of the measures and practices in place.
- Premises are secure when unoccupied.
- There is a contract in place with a data processor which imposes an equivalent security obligation on the data processor.

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

- Clerical and computer procedures are adequate to ensure high levels of data accuracy.
- Appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.

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

- Information held is adequate in relation to the purpose/s for which it is kept.
- Information held is relevant in relation to the purpose/s for which it is kept.
- The information that is held is not excessive in relation to the purpose/s for which it is kept.

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

- Unless where litigation arises (e.g. in relation to accidents/personal injuries involving school personnel/students or accidents occurring on school property), personal data is held for a period of 7 years after the departure of a student or staff member.
- School registers and roll books are required to be kept indefinitely within the school.
- Pay, taxation and related school personnel service records should be retained indefinitely within the school.

8. Give a copy of his/her personal data to that individual on written request and photo identification

An individual on whom the school keeps personal is entitled to:

- a copy of the data which is kept about him/her
- know the purpose/s for processing his/her 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 where such opinions were given in confidence.

To make an access request, an individual must:

- apply in writing
- provide photo identification
- give any details which might be needed to help identify him/her and locate all the information you may keep about him/her

Handling access requests

- There is a named person responsible for handling access requests.
- There is a procedure in place to provide applicants with access to personal data about themselves in accordance with the Data Protection Acts as detailed above.
- On production of a written request and photo identification access will be granted to personal data.
- There is a procedure in place to record the outcome of any legal proceedings which may limit the right of one or both parents to access information about their child.

Note: If spouses are separated and one of them has obtained an order for custody but both of them remain guardians, then both of them are entitled to be involved in important decisions which affect the child.

- A clear co-ordinated procedure is in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is made.
- There is a procedure in place to rectify or erase any inaccurate information as identified by the individual on whom the data is kept, within 40 days of the request being made.
- Information is supplied promptly and in a form which is clear to the ordinary person.

Access requests by students

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

Exceptions to note:

- Data protection regulations prohibit the supply of:
 - health data to a patient in response to a request for access if that would cause serious harm to his or her physical or mental health. The regulations also provide that such data is to be communicated only by, or after consultation with, an appropriate "health professional", normally the patient's own doctor
 - personal data obtained in the course of carrying on social work if that would cause serious harm to the health or emotional condition of the data subject concerned. The regulations apply to social work carried on by Ministers, local

authorities, the HSE or any other such bodies receiving financial assistance from public funds.

Appendix 3 – Procedural Rules for Data Access Request

- An individual is entitled, by law, to be told what information an organisation holds about them, and to be provided with copies of the same. Parents, students and staff can request a copy of information stored about them in the school. This is called a **Data Access Request (DAR)**.
- The School has 40 days to comply with the DAR. There are legal implications for non-compliance.
- All DAR requests must go, initially, via the Principal. These should be considered 'high priority'.
- Upon receipt of an access request, the School is entitled to proof of identity from the requester and to charge a fee of €6.35.
- The Principal and/or Deputy Principal will put together the Information Gathering Team responsible for collating the required information, and assign tasks.
- Marianne B. Matthews of Millett & Matthews Solicitors should be contacted to inform her of the DAR and to seek advice on how best to deal with it.
- Data on individuals may be stored in a variety of different locations, including, but not limited to; VSWare, Filing Cabinets (paper-based), Staff Records. Different staff members will have access to these varied sources and these must be part of the Information Gathering Team. It is the responsibility of these staff members to action the data retrieval from their allocated School Systems, and to keep a note of all steps taken to find and retrieve all the personal data, in case of any subsequent investigation.
- By *day 25* after the DAR, at the latest, the Information Gathering Team should meet and collate all of the relevant information, and prepare it for handover.
- The requester should be supplied with a copy of their personal data in permanent form. This should be a hard-copy printout with any third party information redacted. A copy of all information should be made and retained by the School.
- The information should be handed directly to the individual by the Principal or designate. If this is not possible it should be posted using registered post.
- The School does not store staff information for longer than 7 years past the contract end date.