Rathbeggan N.S.

Dunshaughlin, Co. Meath

Tel: 01 8259891 e-mail: office@rathbegganns.ie

Registered Charity Number: 20131616

DATA PROTECTION POLICY

1 Purpose and Scope

1.1 The purpose of this Data Protection Policy is to support the school in meeting its responsibilities with regard to the processing of personal data. These responsibilities arise as statutory obligations under the relevant data protection legislation. They also stem from our desire to process all personal data in an ethical manner which respects and protects the fundamental rights and freedoms of natural persons.

1.2 This policy aims to help transparency by identifying how the school expects personal data to be treated (or "processed"). It helps to clarify what data is collected, why it is collected, for how long it will be stored and with whom it will be shared.

1.3 The Irish *Data Protection Act (2018)* and the European *General Data Protection Regulation (2016)* are the primary legislative sources.[1] As such they impose statutory responsibilities on the school as well as providing a number of fundamental rights (for students, parents/guardians and staff and others) in relation to personal data.

[1] The school is also cognisant of other legislation which relates to the processing of personal data, whether in manual or in electronic form. For example, the 2011 e-Privacy Regulations (S.I. No. 336 of 2011) provide statutory guidance with regard to certain data processing operations (e.g. direct marketing, cookie notifications on school website etc.).

(vi) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

2.4 GDPR also establishes **Accountability** as a core data processing principle. This places a statutory responsibility on the school, as Data Controller, to be able to demonstrate compliance with the other principles i.e. the 6 data processing principles set out in the previous paragraph (2.3 above).

3 Lawful Basis for Processing Personal Data

3.1 Whenever the school is processing personal data, all of the principles listed in the previous section(s), must be obeyed. In addition, at least one of the following bases (GDPR Article 6) must apply if the processing is to be lawful,

(i) compliance with a legal obligation
(ii) necessity in the public interest
(iii) legitimate interests of the controller
(iv) contract
(v) consent
(vi) vital interests of the data subject.

3.2 When processing **special category personal data**, the school will ensure that it has additionally identified an appropriate lawful basis under GDPR Article 9.[3] Special categories of personal data are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4 Processing Activities Undertaken by the School

4.1 **Record of Processing Activities** This policy sets out the purposes for which the school collects and uses personal data for each of the various categories of data held (student, staff, parent, etc).

4.2 **Student Records** The purposes for processing student personal data include the following: [4]

(i) to provide information prior to application/enrolment;
(ii) to determine whether an applicant satisfies the school's admission criteria;
(iii) to comprehend the educational, social, physical and emotional needs of the student;
(iv) to deliver an education appropriate to the needs of the student;
(v) to ensure that any student seeking an exemption from Irish meets the criteria;
(vi) to ensure that students benefit from relevant additional educational or financial supports;
(vii) to contact parents/guardians in case of emergency or in the case of school closure;
(viii) to monitor progress and to provide a sound basis for advising students and parents/guardians;
(ix) to inform parents/guardians of their child's educational progress etc.;
(x) to communicate information about, and record participation in, school events etc.;
(xi) to compile yearbooks, establish a school website, and to keep a record of the history of the school;
(xii) to comply with legislative or administrative requirements;
(xiii) to furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and others in compliance with law and directions issued by government departments.

---

[3] GDPR Article 9 sets out the lawful bases that apply to the processing of special categories of personal data.

[4] Appendix 5 sets out the type of personal data being processed by the school and the purposes for which this data is being processed. This list is likely to be subject to revision from time to time. For example, changes in curriculum or legislation may require adjustments in the personal data processing.

Department of Education and Skills. As such their actions will be governed by national and European data protection legislation as well their own organisational policies.[5]

(iv) Some of the school's operations require support from specialist service providers. For example, the school may use remote IT back-up and restore services to maintain data security and integrity. In cases such as these, where we use specialist data processors, we will ensure that the appropriate security guarantees have been provided and that there is a signed processing agreement in place.

6 Personal Data Breaches

6.1 **Definition of a Personal Data Breach** A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

6.2 **Consequences of a Data Breach**

(i) A breach can have a significant adverse effect on individuals, which can result in physical, material or non-material damage. This can include discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality etc. Children, because of their age, may be particularly impacted.

(ii) In addition to any detrimental impact on individual data subjects, a data breach can also cause serious damage to the school. This can include reputational damage as well as exposing the school to other serious consequences, including civil litigation.

(iii) It should be noted the consequences of a data breach could include disciplinary action, criminal prosecution and financial penalties or damages for the school and participating individuals.[6]

6.3 **Responding to a Data Breach**

(i) The school will always act to prioritise and protect the rights of those individuals whose personal data is affected.

(ii) As soon as the school becomes aware that an incident has occurred, measures will be taken to assess and address the breach appropriately, including actions to mitigate any possible adverse effects.

(iii) Where the school believes that there is a risk to the affected individuals, the school will (within 72 hours of becoming aware of the incident) submit a report to the Data Protection Commission.

(iv) Where a breach is likely to result in a high risk to the affected individuals, the school will inform those individuals without undue delay.

7 Data Subject Rights

7.1 **Your Rights** Personal Data will be processed by the school in a manner that is respectful of the rights of data subjects. Under GDPR these include[7]

(i) the right to information
(ii) the right of access
(iii) the right to rectification
(iv) the right to erasure ("right to be forgotten")
(v) the right to restrict processing
(vi) the right to data portability
(vii) the right to object
(viii) the right not to be subject to automated decision making
(ix) the right to withdraw consent
(x) the right to complain.

---

[5] The Data Protection Policy of the Department of Education and Skills can be viewed on its website (www.education.ie).

[6] The Data Protection Act 2018 established a number of offences whereby breaches of the Act can result in fines and/or imprisonment.

[7] For further information on your rights see www.GDPRandYOU.ie.

Telephone	+353 57 8684800
	+353 (0)761 104 800
Lo Call Number	1890 252 231
Fax	+353 57 868 4757
E-mail	info@dataprotection.ie
Post	Data Protection Commission
	Canal House, Station Road
	Portarlington, Co. Laois
	R32 AP23
Website	www.dataprotection.ie

Appendix 2. IMPLEMENTING THE DATA PROCESSING PRINCIPLES

1. Accountability

(i) Accountability means that compliance with the data protection legislation is recognised as an important Board of Management responsibility as well as one shared by each school employee and member of the wider school community.[10]

(ii) Demonstrating Compliance Accountability imposes a requirement on the controller to demonstrate compliance with the other data processing principles (see Section 2 earlier: *Processing Principles*). This means that the school retains evidence to demonstrate the actions it has taken to comply with GDPR.

(iii) School Policies An important way for the school to demonstrate accountability is through the agreement and implementation of appropriate policies. In addition to publishing a *Data Protection Policy* this may include developing other policies to address some or all of the following areas(i) Data Breaches (ii) Data Access Requests (iii) Record Storage and Retention (iv) Data Processing Agreements.[11]

(iv) Record of Processing Activities As a data controller the school is required to prepare a record of any processing activities (ROPA) that it undertakes. This record should include the following information (GDPR Article 30):

- the purposes of the processing;
- a description of the categories of data subjects and personal data;
- the categories of recipients to whom the personal data will be disclosed;
- any transfers to a third country or international organisation, including suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures.

(v) Risk Assessment The school as data controller is required to consider any risks that may arise as a consequence of its processing activities. This assessment should consider both the likelihood and the severity of these risks and their potential impact on data subjects.[12]

(vi) Data Protection Impact Assessment (DPIA) A DPIA is a type of risk assessment that is mandatory in specific circumstances (GDPR Article 35). The school will ensure that a DPIA is undertaken where this is appropriate, typically, where a new processing activity has the potential to have a high impact on individual privacy or rights. The purpose of undertaking a DPIA is to ensure that any risks associated with the new processing activity are identified and mitigated in an appropriate manner.

(vii) Security of Processing As a consequence of having assessed the risks associated with its processing activities, the school will implement appropriate *technical and organisational measures* to ensure a level of security appropriate to the risk. For example, these measures might include training of

---

[10] The GDPR4schools.ie website identifies some of the GDPR Roles and Responsibilities held by different groups, namely (i) Board of Management (ii) Principal/Deputy Principal (iii) Teaching Staff (iv) Guidance & Medical Support (v) School Administration (vii) SNAs and (viii) Caretaker. These lists of responsibilities (provided in PDF format) can be shared out to help raise awareness amongst the school community.

[11] All school policies need be applied in a manner that respects the principles, protocols and procedures inherent in the school's Data Protection strategy. Examples of relevant policies include (i) Acceptable Use Policy (ICT) (ii) Child Safeguarding Statement (iii) Code of Behaviour (iv) Policy on Special Education Needs (vi) Anti-Bullying Policy.

[12] GDPR Recital 75: The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

3. Consent

Where consent is relied upon as the appropriate condition for lawful processing, then that consent must be freely given, specific, informed and unambiguous. All of these conditions must be satisfied for consent to be considered valid. There are a significant number of restrictions around using consent.

(i) A separate consent will be sought for each processing activity (together with appropriate guidance as necessary to ensure the data subject is informed).

(ii) When asking for consent, the school will ensure that the request is not bundled together with other unrelated matters.

(iii) Consent requires some form of clear affirmative action (Silence or a pre-ticked box is not sufficient to constitute consent). Consent can be provided by means of an oral statement.

(iv) Consent must be as easy to withdraw as to give.

(v) A record should be kept of how and when consent was given.

(vi) The school will take steps to ensure the consent is always freely given i.e. that it represents a genuine choice and that the data subject does not feel under an obligation to consent to processing.

(vii) If the consent needs to be explicit, this means the school must minimise any future doubt about its validity. This will typically require the school to request and store a copy of a signed consent statement.

4. Special Category Data

Some personal data is defined as Special Category Data and the processing of such data is more strictly controlled. In a school context this will occur whenever data that relates to Special Needs or Medical Needs is being processed. GDPR Article 9 identifies a limited number of conditions, one of which must be applicable if the processing of special category data is to be lawful.[17] Some of these processing conditions, those most relevant in the school context, are noted here.

(i) Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law. This condition could provide an appropriate basis for processing of data relating to employee and student health e.g. proportionate sharing of special category data to ensure the school is compliant with provisions in health, safety and welfare legislation.

(ii) Processing is necessary for the assessment of the working capacity of an employee;....or for the provision of health or social care or treatment.. on the basis of Union or Member State law.

5. Transparency

The school as Controller is obliged to act with *Transparency* when processing personal data. This requires the communication of specific information to individuals in advance of any processing of their personal data.[18]

(i) Transparency is usually achieved by providing the data subject with a written document known as a *Privacy Notice* or a *Privacy Statement*.[19] This notice will normally communicate:

- the name of the controller and their contact details;
- the categories of personal data being processed;
- the processing purposes and the underlying legal bases;
- any recipients (i.e. others with whom the data is shared/disclosed);
- any transfers to countries outside the EEA (and safeguards used);
- the storage period (or the criteria used to determine this);

[17] The Data Protection Act 2018 makes provision for some additional conditions that can legitimise the processing of special category data.

[18] GDPR Articles 13 (or 14)

[19] Other terms in common use include *Fair Processing Notice* and *Data Protection Notice*. Schools may prepare a number of different Privacy Notices for use in different contexts. For example, a *Website Privacy Notice*, may relate specifically to personal data that is collected via the school website.

8. Storage Limitation

Personal data is kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which it is being processed. Some personal data may be stored for longer periods insofar as the data is being processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(i) When deciding on appropriate retention periods, the school's practices will be informed by advice published by the relevant bodies (notably the Department of Education and Skills, the Data Protection Commission, and the school management advisory bodies[24]).

(ii) When documentation or computer files containing personal data are no longer required, the information is disposed of in a manner that respects the confidentiality of the data.

(iii) Data subjects are free to exercise a "right to erasure" at any time (also known as the "right to be forgotten", see *Data Subject Rights*).

(iv) Data should be stored in a secure manner that recognises controller obligations under GDPR and the Data Protection Act. This requires the school for example, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

9. Integrity and Confidentiality

Whenever personal data is processed by the school, technical and organisational measures are implemented to safeguard the privacy of data subjects. The school as controller is obliged to take its security responsibilities seriously, employing the most appropriate physical and technical measures, including staff training and awareness. These security procedures should be subject to regular review.

(i) School employees are required to act at all times in a manner that helps to maintain the confidentiality of any data to which they have access. Guidance and training are important to help identify and reinforce appropriate protocols around data security.

(ii) The school is legally required to consider the risks to the data subject when any processing of personal data is taking place under its control. Any Risk Assessment should take particular account of the impact of incidents such as accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, the personal data.

(iii) As well considering the potential severity of any data incident, a risk assessment should also consider the likelihood of any incident occurring. In this way risks are evaluated on the basis of an objective assessment, by which it is established whether the data processing operations involve a risk or a high risk.[25]

(iv) The follow-on from any risk assessment is for the school to implement appropriate technical and organisational measures that ensure a level of security appropriate to the risk. *These measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected (GDPR Recital 83).*

(v) As well as processing activities undertaken by staff, the school must also consider the risks associated with any processing that is being undertaken on behalf of the school by other individuals or organisations (Data Processors). Only processors who provide sufficient guarantees about the implementation of appropriate technical and organisational measures can be engaged.

---

[24] see http://www.dataprotectionschools.ie/en/Data-Protection-Guidelines/Records-Retention/

[25] The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk (GDPR Recital 76).

Appendix 3. CATEGORIES OF RECIPIENTS

Department of Education and Skills (DES) The school is required to provide student data to the *Department of Education and Skills (DES).* This transfer of data is primarily made at the beginning of each academic year ("October Returns") using a secure Primary Online Database (POD) system. The October Returns contain individualised data such as PPS number which acts as an identifier to validate that the data belongs to a recognised student.[26] The DES has published a "Fair Processing Notice" to explain how the personal data of students is processed.[27]

Student support and welfare student data may be shared with a number of public state bodies including *National Educational Psychological Service* (NEPS psychologists support schools and students); *National Council for Special Education* (the NCSE role is to support schools and students with special education needs); *National Education Welfare Board* (the school is required to share student attendance with the NEWB).

Legal requirements where appropriate, particularly in relation to Child Protection and safeguarding issues, the school may be obliged to seek advice and/or make referrals to *Túsla.*[28] The school may share personal data with *An Garda Síochána* where concerns arise in relation to child protection. The school will also report matters of alleged criminal acts, criminal behaviour, criminal damage, etc., to allow prevention, detection and investigation of offences. Where there is a lawful basis for doing so, personal data may also be shared with the *Revenue Commissioners* and the *Workplace Relations Commission.*

Insurance data may be shared with the school's insurers where this is appropriate and proportionate. The school may also be obliged to share personal data with the *Health and Safety Authority*, for example, where this is required as part of an accident investigation.

Professional Advisors some data may be shared with legal advisors (solicitors, etc.), financial advisors (pension administrators, accountants, etc.) and others such as school management advisors; this processing will only take place where it is considered appropriate, necessary and lawful.

Other schools where the student transfers to *another educational body*, the school may be asked to supply certain information about the student, such as academic records etc. Note: Education Passport (6th Class Report) provided to post-primary school, after the post-primary school confirms enrolment. These protocols are set out in DES Circulars 0042/2015, 0034/2016 and Circular 0056/2011 (Initial Steps in the Implementation of the National Literacy and Numeracy Strategy).

Voluntary Bodies some personal data may be shared as appropriate with bodies such as the school's *Parents Association*. This data sharing will only take place where consent has been provided.

Other not-for-profit organisations limited data may be shared with recognised bodies who act to promote student engagement with co-curricular and other activities, competitions, recognition of achievements, etc. This would include bodies promoting participation in sports, arts, sciences, environmental and outdoor activities, etc. This data sharing will usually be based on consent.

---

[26] Where the October Returns include sensitive personal data regarding personal circumstances then explicit and informed consent for the transfer of this data may be sought from students/parents/guardians.

[27] These can be found on www.education.ie (search for Circular Letter 0037/2016 in the "Circulars" section and Fair Processing Notice September 2015). The Department of Education and Skills transfers some student 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.

[28] Túsla, the Child and Family Agency, is the State agency responsible for improving wellbeing and outcomes for children.

Appendix 4. MANAGING RIGHTS REQUESTS

1. Responding to rights requests

(i) The school will log the date of receipt and subsequent steps taken in response to any valid request. This may include asking the data subject to complete an *Access Request Form* in order to facilitate efficient processing of the request. There is no charge for this process.[29]

(ii) The school is obliged to confirm the identity of anyone making a rights request and, where there is any doubt on the issue of identification, will request official proof of identity (e.g. photographic identification such as a passport or driver's licence).[30]

(iii) If requests are manifestly unfounded or excessive[31], in particular because of their repetitive character, the school may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or refuse to act on the request.

(iv) The school will need to confirm that sufficient information to locate the data requested has been supplied (particularly if CCTV footage/images are to be searched[32]). Where appropriate the school may contact the data subject if further details are needed.

(v) In responding to rights requests (e.g. data access requests) the school will ensure that all relevant manual[33] and automated systems (computers etc.) are checked.

(vi) The school will be conscious of the need to respond without undue delay and within the advised timeframes. A response will be made within one month of receipt of any request.[34]

(vii) The school must be conscious of the restrictions that apply to rights requests.[35] Where unsure as to what information to disclose, the school reserves the right to seek legal advice.[36]

(viii) Where a request is not being fulfilled, the data subject will be informed as to the reasons and the mechanism for lodging a complaint, including contact details for the Data Protection Commission.

(ix) Where action has been taken by the school with regard to rectification, erasure or restriction of processing, the school will ensure that relevant recipients (i.e. those to whom the personal data has been disclosed) are appropriately informed.

2. Format of Information supplied in fulfilling a request

(i) The information will be provided in writing, or by other means, including where appropriate, by electronic means. (When requested by a data subject the information access may be provided in alternative means e.g. orally.)

(ii) The school will endeavour to ensure that information is provided in an intelligible and easily accessible format.

---

[29] The school may charge a reasonable fee for any further copies requested by the data subject, or where access requests are manifestly unfounded or excessive, taking into account the administrative costs of providing the information. 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.

[30] Where a subject access request is made via a third party (e.g. a solicitor) the school will need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement.

[31] In such circumstances, the school must be able to demonstrate the manifestly unfounded or excessive character of a request.

[32] The school will always endeavour to respond to any access request within the stipulated time period. However a timely response can be greatly facilitated by provided (in writing to the school) all necessary information such as date, time and location of any recording.

[33] Non-automated personal data that is held within a filing system or intended to form part of a filing system (GDPR Article 2).

[34] That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The school must inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

[35] See for example GDPR Article 23 and Irish Data Protection Act 2018 S.56, S.60, S.61.

[36] Decisions around responding to data access requests will need to give due regard to rights and responsibilities that derive from other legislation, not least Article 42A of the Irish Constitution which recognises and affirms the natural and imprescriptible rights of all children. Examples of other factors that might need to be considered include: any court orders relating to parental access or responsibility that may apply; any duty of confidence owed to the child or young person; any consequences of allowing those with parental responsibility access to the child's or young person's information (particularly important if there have been allegations of abuse or ill treatment); any detriment to the child or young person if individuals with parental responsibility cannot access this information; and any views the child or young person has on whether their parents should have access to information about them.

Appendix 5. PERSONAL DATA AND RELATED PROCESSING Purposes

PURPOSES FOR PROCESSING	DESCRIPTION OF PERSONAL DATA
1. Contact and identification information This information is needed to identify, contact or enrol students.	
Purposes may include: • to add names to a contact list prior to formal application • to provide appropriate information to prospective students • to make contact in case of school closure (e.g. adverse weather conditions) • to send SMS text messages and emails about meetings, etc.	Information required to confirm student/parent identity and contact through communications: • student name • gender • date of birth • family details (parents/guardians name, address, contact details to include phone numbers, email addresses etc).
2. Application information We use this to determine whether an applicant meets eligibility requirements as set out in our Admission Policy.	
In addition to data outlined at (1) above, we collect personal data via Application Forms and Student Transfer Forms. Where the student is offered a place, completed Application Forms are placed on the student's file. Where the student is not offered a place, the data will be used for the purposes of responding to any section 29 appeals process. Applicants may opt to provide data on "Religion" at this stage where this forms part of the school's admissions criteria. Any information not required to operate the Admissions Procedure, is identified as optional.	Information as required to ascertain eligibility under the school's Admissions Policy: • Name and address of current school • Class in current school • Details of siblings, etc. • Details of any special educational needs (SEN). (NB only for admission to a special school, or a SEN unit). • Language: details re Irish language. (Gaelscoil / Gaelcholáiste only) • Religion (based on consent) Note: Religion may no longer be used in Catholic schools as a criterion for school admission.
3. Enrolment information Once the school has accepted the student's application, and has offered the student a place, other information is collected in addition to the data outlined at (1) and (2) above. This personal data is used for administrative and management tasks e.g. school communications, timetabling, scheduling parent teacher meetings, school events, class details, start dates, book lists, school trips etc.	
Contact and Identification Information: We use this information: • to make contact in case of school closure (e.g. adverse weather conditions), or an emergency (ill-health or injury), • to communicate issues relating to progress, welfare or conduct in school, non-attendance or late attendance, etc. • to send SMS text messages and emails about important events, e.g. start dates, course details, meetings, school events, etc.	• Student name and date of birth (requires birth certificate verification by school) • PPSN, Gender • Address including Eircode • Extended family details (parents/guardians name, address, contact details to include phone numbers, email addresses etc). • Details of next of kin (for contact in case of emergency)
Academic record: We use this information to deliver education appropriate to the needs of the student, to assess the student's educational progress. Standardised test results used for the purposes of assessing literacy/numeracy progress, for assisting in referrals to NEPS etc.	• Reports, references, assessments and other records from any previous school(s) attended by the student. • Academic information provided from one school to another after the new school confirms enrolment. Protocols are set out in DES Circular 0056/2011 • Standardised testing Results
Language spoken: Without this information the school will not know how to meet the student's needs and to deliver appropriate education. This ensures the student has access to language support (where necessary). Irish Exemption Information re application for Irish exemption if eligible (e.g. received primary school up to 11 years of age outside Ireland, evidence of disability, student from abroad etc).	• Information about language spoken (for language support) • Details of whether the student received EAL (English as an Additional Language) support. • Details re whether the student is exempt from studying Irish • Details to ascertain if student is eligible for exemption from study of Irish
Medical information for health purposes: This information is essential so that we can meet our duty of care to the student. We use this information to (i) ensure we know who to contact in case of an emergency, (ii) ensure that we have any relevant information to safeguard/prevent damage to the student's health (iii) meet the student's medical/care needs when they are in school (iv) facilitate appropriate advanced planning with	• Emergency contact details (name, telephone, details of relationship to the student etc). • Details of the student's GP (to be contacted in case of emergency). • Details of any relevant medical information (e.g. medical condition, allergies, treatment/care plan etc) to facilitate appropriate advanced planning with parents/guardians.

CCTV images: The school processes this data for the purposes outlined in our CCTV Policy, a copy of which is available on the school's website e.g. *We use CCTV for security purposes; to protect premises and assets; to deter crime and anti-social behaviour; to assist in the investigation, detection, and prosecution of offences; to monitor areas in which cash and/or goods are handled; to deter bullying and/or harassment; to maintain good order and ensure the school's Code of Behaviour is respected; to provide a safe environment for all staff and students; for verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and the recordings may be capable of resolving that dispute; for the taking and defence of litigation.*	CCTV is in operation at the perimeter, exterior and certain internal common areas within the school both during the daytime and during the night hours each day. CCTV is used at external points on the premises (eg. at front gates, in the car-park etc) and at certain internal points (eg. front desk/reception area, corridors etc). In areas where CCTV is in operation, appropriate notices will be displayed.
Special needs data, educational support records, medical data etc: Without this information, the school will not know what resources need to be put in place in order to meet the student's needs and to deliver appropriate education in-keeping with its statutory obligations. This is in order to assess student needs, determine whether resources can be obtained and/or made available to support those needs, and to develop individual education plans. 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 (the statutory agency established under the Education for Persons with Special Educational Needs Act 2004) such information as the Council may from time to time reasonably request.	The school collects information relating to any special educational needs, psychological assessments/reports, information about resource teaching hours and/or special needs assistance hours, etc. Schools are also required to share this personal data with SENOs employed by the NCSE. • Psychological assessments, • Special Education Needs' files, reviews, correspondence • Individual Education Plans, • Special Education support file, • Notes relating to inter-agency meetings, • Medical information (including details of any medical condition and/or medication/treatment required) • Psychological, psychiatric and/or medical assessments
Child protection, child welfare records: The school is required to follow DES Child Protection Procedures (Circular 81/2017) and to take appropriate action to safeguard the welfare of students in its care (Child Protection Procedures for Primary and Post-Primary Schools 2017). Staff have a legal responsibility to report actual or suspected child abuse or neglect to the Child & Family Agency ("TUSLA") and to An Garda Síochána. Mandatory reporting obligations arise under Children First 2015, the Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012.	Mandatory reporting obligations require data sharing with TUSLA, An Garda Síochána and any other appropriate law enforcement or child protection authorities. DES Inspectorate may seek access to the school's child protection records for audit and Child Protection and Safeguarding Inspection purposes. • Child protection records • Child safeguarding records • Other records relating to child welfare • Meitheal meetings convened by TUSLA
Pastoral Care Records: This information is required to provide access to psychological services and to provide supports to students, resolve behavioural, motivational, emotional and cognitive difficulties through assessment and therapeutic intervention, to engage in preventative work etc. Personal data (and special category personal data) will be shared with third parties (e.g. TUSLA, NEPS, CAMHS, An Garda Síochána, Medical practitioners treating the student) for the purpose of the school complying with its legal obligations and/or in the student's vital/best interests.	• Record of behavioural concerns including frequency, persistence, context, and intensity of behaviours • Psychological service notes • Referrals to/records relating to therapeutic services and other interventions • Minutes, notes and other records concerning Student Support
Internal school processes: This information (e.g. anti-bullying processes and disciplinary/Code of Behaviour processes) is required to meet the school's duty of care to all its students and staff, to comply with relevant Circulars issued by the Department of Education and Skills, and to run the school safely and effectively. Data collected in these processes may be transferred to the school's insurer and/or legal advisors or management body as appropriate where required for disputes resolution, fact verification, and for litigation purposes.	• Records of parental complaints. • Records of other complaints (student to student complaints etc). • Records relating bullying investigations. • Records relating to Code of Behaviour processes (expulsion, suspension etc.) including appeals data and section 29 appeals material.
Accident and injury reports: This information is processed to operate a safe environment for students and staff, to identify and mitigate any potential risks, and to report incidents/accidents. This data may be transferred to the school's insurance company and/or indemnifying body and/or legal advisors as appropriate. Data will be shared with An Garda Síochána, TUSLA and the Health & Safety Authority where appropriate.	• Accident reports • Incident Report Forms • Notifications to insurance company • Exchanges with legal advisors. • Notifications to Health & Safety Authority (HSA)

Appendix 6. REFERENCE SITES

Data Protection Act 2018 http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

General Data Protection Regulation (GDPR official text) 2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj

General Data Protection Regulation (GDPR unofficial web version) 2016 https://gdpr-info.eu/

GDPR for Schools website https://gdpr4schools.ie/

Data Protection for Schools http://dataprotectionschools.ie/en/

Irish Data Protection Commission https://www.dataprotection.ie/

Data Breach Report https://forms.dataprotection.ie/report-a-breach-of-personal-data

European Data Protection Board (EDPB) https://edpb.europa.eu/

EDPB Guidelines, Recommendations and Best Practices on GDPR https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

PDST Technology in Education https://www.pdsttechnologyineducation.ie

Cyber Security Centre (Ireland) https://www.ncsc.gov.ie/

Cyber Security Centre (UK) https://www.ncsc.gov.uk/