Villiers School

DATA PROTECTION POLICY

In compliance with General Data Protection Regulation (GDPR)

February 2020

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 safe 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.

1.4 The school recognises the seriousness of its data processing obligations and has implemented a set of practices to safeguard personal data. Relevant policies and procedures apply to all school staff, boards of management, trustees, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school).

[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.).

1.5 Any amendments to this Data Protection Policy will be communicated through the school website and other appropriate channels, including direct communication with data subjects where this is appropriate. We will endeavour to notify you if at any time we propose to use Personal Data in a manner that is significantly different to that stated in our Policy, or, was otherwise communicated to you at the time that it was collected.

1.6 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. Formally, the statutory responsibility of Controller is assigned to the Boards of Governors and Management as appropriate ("the Board of Management"). The Headmistress is assigned the role of co-ordinating the implementation of this Policy and for ensuring that all staff who handle or have access to Personal Data are familiar with their responsibilities.

Name	**Responsibility**
Board of Management	Data Controller
Headmistress	Implementation of Policy
All Staff	Adherence to the Data Processing Principles
Entire School Community	Awareness and Respect for all Personal Data

2 Processing Principles

2.1 **Processing** is the term used to describe any task that is carried out with personal data e.g. collection, recording, structuring, alteration, retrieval, consultation, erasure as well as disclosure by transmission, dissemination or otherwise making available. Processing can include any activity that might relate to personal data under the control of the school, including the storage of personal data, regardless of whether the records are processed by automated or manual means.

2.2 There are a number of fundamental principles, set out in the data protection legislation, that legally govern our treatment of personal data. As an integral part of its day to day operations, the school will ensure that all data processing is carried out in accordance with these processing principles.

2.3 These principles, set out under GDPR, establish a statutory requirement that personal data must be:

(i) processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**);

(ii) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes **(purpose limitation)**;

(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**);

(iv) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**accuracy**);

(v) kept for no longer than is necessary for the purposes for which the personal data are processed[2]; (**storage limitation**);

(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;

[2] Data may be stored for longer periods if being processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (subject to appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject).

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

[4] Appendix 2 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.

(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 State Exams Commission, the National Council for Special Education, TUSLA, and others in compliance with law and directions issued by government departments.
(xiv) to facilitate school trips such as MUN, ski trip, Music Trip, Cross Curricular trip, exchanges, etc
(xv) to celebrate school and pupil achievements, to record in media and social media sites such as Red Sokz, the school magazine, yearbooks, the school website, twitter, instagram, alumni and friends facebook page, newslink, local media, national media.

4.3 **Parent / Guardian Records** The school does not keep personal files for parents or guardians. However, information about, or correspondence with, parents may be held in the files for each student. This information shall be treated in the same way as any other information in the student file. The School keeps financial records which include records of fee statements and payment history. These records are administered by the Bursar's office and are treated as strictly confidential. Parents are entitled to contact the school to seek details of their financial record, and shall be facilitated in such a way that the financial record of no other parent or family is divulged. The School is fully audited each year and as part of this process all financial information, including fee statements, are made available to the School auditors. This information is treated as strictly confidential by the auditors. Relevant data is also passed onto the school's solicitor in the event of non-cooperation and or / non-payment of fees and / or in cases of dispute or law. The school, where relevant, will liaise in a strictly confidential manner, with the secondary education committee (SEC) in relation to SEC grant applications.

4.4 **Staff Records** As well as records for existing members of staff (and former members of staff), records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. The purposes for which staff personal data is processed include the following:
(i) the management and administration of school business (now and in the future);
(ii) 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);
(iii) to facilitate pension payments in the future;
(iv) human resources management;
(v) recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.;

(vi) 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*);

(vii) 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;

(viii) and for compliance with legislation relevant to the school.

4.5 **Board of Management Records** Board of Management records are kept in accordance with the Education Act 1998 and other applicable legislation. Minutes of Board of Management meetings record attendance, items discussed and decisions taken. Board of Management business is considered confidential to the members of the Board.

4.6 **Financial Records** This information is required for routine management and administration of the school's financial affairs, including the payment of fees, invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

4.7 **CCTV Records** The school processes personal data in the form of recorded CCTV images. We use CCTV for the following purposes:

(i) to secure and protect the school's premises and assets;

(ii) to deter crime and anti-social behaviour;

(iii) to assist in the investigation, detection, and prosecution of offences;

(iv) to monitor areas in which cash and/or goods are handled;

(v) to deter bullying and/or harassment;

(vi) to maintain good order and ensure the school's Code of Behaviour is respected;

(vii) to provide a safe environment for all staff and students;

(viii) for the taking and defence of litigation;

(ix) for verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and where the recordings may be capable of resolving that dispute.

5 Recipients

5.1 **Recipients** These are defined as organisations and individuals to whom the school transfers or discloses personal data. Recipients may be data controllers, joint controllers or processors. A list of the categories of recipients used by the school is provided in the appendices (Appendix 3). This list may be subject to change from time to time.

5.2 **Data Sharing Guidelines**

(i) From time to time the school may disclose Personal Data to third parties, or allow third parties to access specific Personal data under its control. An example could arise should Gardai submit a valid request under Section 41(b) of the Irish Data Protection Act which allows for *processing necessary and proportionate for the purposes of preventing, detecting, investigating or prosecuting criminal offences.*

(ii) In all circumstances where personal data is shared with others, the school will ensure that there is an appropriate lawful basis in place (GDPR Articles 6, 9 as appropriate). We will not share information with anyone without consent unless another lawful basis allows us to do so.

(iii) Most data transfer to other bodies arises as a consequence of legal obligations that are on the school, and the majority of the data recipients are Controllers in their own right, for example, the 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]

[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.

(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.

7.2 **Right to be Informed** You are entitled to information about how your personal data will be processed. We address this right primarily through the publication of this Data Protection Policy. We also publish additional privacy notices/statements which we provide at specific data collection times, for example, our Website Data Privacy Statement is available to all users of our website. Should you seek further clarification, or information that is not explicit in our Policy or Privacy Statements, then you are requested to forward your query to the school.

7.3 **Right of Access** You are entitled to see any information we hold about you. The school will, on receipt of a request from a data subject, confirm whether or not their personal data is being processed. In addition, a data subject can request a copy of their personal data. The school in responding to a right of access must ensure that it does not adversely affect the rights of others.

7.4 **Right to rectification** If you believe that the school holds inaccurate information about you, you can request that we correct that information. The personal record may be supplemented with additional material where it is adjudged to be incomplete.

7.5 **Right to be forgotten** Data subjects can ask the school to erase their personal data. The school will act on such a request providing that there is no compelling purpose or legal basis necessitating retention of the personal data concerned.

7.6 **Right to restrict processing** Data subjects have the right to seek a restriction on the processing of their data. This restriction (in effect requiring the controller to place a "hold" on processing) gives an individual an alternative to seeking erasure of their data. It may also be applicable in other circumstances such as where, for example, the accuracy of data is being contested.

7.7 **Right to data portability** This right facilitates the transfer of personal data directly from one controller to another. It can only be invoked in specific circumstances, for example, when processing is automated and based on consent or contract.

7.8 **Right to object** Data subjects have the right to object when processing is based on the school's legitimate interests or relates to a task carried out in the public interest (e.g. the processing of CCTV data may rely on the school's legitimate interest in maintaining a safe and secure school building). The school must demonstrate compelling legitimate grounds if such processing is to continue.

7.9 **Right not to be subject to automated decision making** This right applies in specific circumstances (as set out in GDPR Article 22).

7.10 **Right to withdraw consent** In cases where the school is relying on consent to process your data, you have the right to withdraw this at any time, and if you exercise this right, we will stop the relevant processing.

7.11 **Limitations on Rights** While the school will always facilitate the exercise of your rights, it is recognised that they are not unconditional: the school may need to give consideration to other obligations.[8]

7.12 **Right to Complain**

(i) If you are concerned about how your personal data is being processed, then please address these concerns in the first instance to the Headmistress who is responsible for operational oversight of this policy.[9]

(ii) A matter that is still unresolved may then be referred to the school's Data Controller (i.e., the Board of Management) by writing to the Chairperson c/o school.

(iii) Should you feel dissatisfied with how we have addressed a complaint or concern that you have raised, you have the right, as data subject, to bring the matter to the attention of the Irish Data Protection Commission.

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

[8] See GDPR Articles 12-23 for a full explanation of subject rights and their application.

[9] Parents/Guardians may also, where applicable, have the option of invoking the school's formal complaints procedure (available from school).

Appendix 1. GLOSSARY

Child - a person under the age of 18 years. Children are deemed as vulnerable under GDPR and merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Controller or **Data Controller** - an entity or person who, alone or jointly with others, determines the purposes and means of the processing of personal data. In this policy, the data controller is the School.

Consent - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Protection Commission - the national supervisory authority responsible for monitoring the enforcing the data protection legislation within Ireland. The DPC is the organisation to which schools as data controllers must notify data breaches where there is risk involved.

Data Protection Legislation – this includes (i) the General Data Protection Regulation (GDPR) - *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, and (ii) the Irish Data Protection Act (2018). GDPR is set out in 99 separate *Articles*, each of which provides a statement of the actual law. The regulation also includes 171 Recitals to provide explanatory commentary.

Data Subject - a living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

Data concerning health - personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. This is an example of special category data (as is data concerning special education needs).

Personal data - any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach - 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.

Processing - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor or **Data Processor** - a person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract (<u>but does not include</u> an employee of a controller who processes such data in the course of his or her employment).

Profiling - any form of automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

(Relevant) Filing System - any set of information that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

Special categories of data - personal data 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.

Appendix 2. 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 and 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)
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, arrangements for academic registration, class details, start dates, book lists, subject-selection, 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,	• Student name and date of birth (requires birth certificate verification by school) • PPSN, Address including Eircode • Extended family details (parent/guardian names, contact details, postal & email address, phone numbers, addresses, details of any court orders or other arrangements governing access to, or custody of, child). • Details of next of kin (for contact in case of emergency)

meetings, school events, etc.	
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 Reasonable Accommodation in State Examinations, for assisting in referrals to NEPS, and for career guidance etc.	• Reports, references, assessments and other records from any previous school(s) attended by the student. • Education Passport (6th Class Report provided by primary school after post-primary school confirms enrolment. Protocols set out in DES Circulars 42/2015 and 34/2016). • 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 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 to meet our duty of care to the student. We use this information to (i) ensure we know who to contact in case of emergency, (ii) ensure that we have relevant information to safeguard/prevent damage to student health (iii) meet medical/care needs when students are in school (iv) facilitate appropriate advanced planning with parents/guardians (e.g. notification to relevant personnel within the school, storage of medications, staff training where necessary etc).	• 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. This may include use of student's photograph for display in the Staff room as part of the emergency action plan.

SEN and Medical information for educational purposes: We cannot meet our duty of care to the student and our obligations under EPSEN Act 2004 without this information. We use this information to (i) make application to the DES for allocation of resources to support student (ii) ensure school has relevant information to deliver education appropriate to student's needs (iii) apply for appropriate accommodation(s) and/or therapeutic supports where available.	• Details of any special needs/medical needs that need to be accommodated, e.g. medical assessment, hearing/vision issues, psychological assessment/report. • Details of whether the student has been in receipt of learning support. • Details of whether the student been granted resource teaching hours and/or special needs assistance hours by the NCSE.
Information sought by Department of Education and Skills (DES): We are under a legal obligation to return specific enrolment information concerning each student to DES (SI 317/2015). This data is used to calculate teacher and resource allocation, capitation, grant payments for schools, for statistical analysis and reporting in the areas of social inclusion and integration of students in the education system, and for planning purposes. Other (optional) information is sought for purposes relating to planning, social inclusion and integration of students in the education system.	Personal data is transferred to the DES via the Post-Primary Online Database as set out in the Privacy Notice for P-POD provided by DES. Required information includes, e.g. birth name of student and mother (to verify student identity). The DES seeks some additional information on an optional basis (i.e. based on parental consent), for example, • Ethnic/Cultural background
Use of photographs for yearbooks, social media, website etc.: Photographs, and recorded images of students may be taken at school events and to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school.	• Consent to use (for these purposes) images or recordings in printed or digital format. • Separate consents will be sought for different publication forums. (NB This excludes CCTV recordings - see school CCTV policy).
Religion only sought where the school facilitates religious instruction/faith formation at the request of parent(s)/ guardian(s).	• Religious denomination (based on consent)
Consents to direct marketing: If you wish to receive direct marketing you can give consent for us to contact you by SMS text and/or email. Your right to opt-out only relates to the school contacting you for direct marketing purposes.	Note: We will still contact you on your mobile in case of an emergency relating to your child and/or to communicate messages about school events (e.g. school closure, parent-teacher meetings etc).
4. Personal data gathered during student's time in School We cannot meet our statutory obligation to deliver appropriate education to students and/or we cannot satisfy our duty of care to each student without processing this information.	
Academic progress: The school processes this personal data in order to deliver education to students, and to evaluate students' academic progress, to register the student for State Examinations (Junior Cycle, Leaving Cycle), to submit the students' work to the recognised accrediting body etc.	• Academic progress and results • State exam results • Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results) • Continuous assessment and end of term/year reports

Attendance: The school is required to collect and monitor attendance data and to notify the Education Welfare Officer (TUSLA) in certain circumstances, such as (i) where the student is suspended for 6 days or more (ii) where the student is absent for an aggregate period of 20 school days during the course of the year, (iii) where the Headmistress is of the opinion that the student is not attending school regularly. The school will notify parent/guardian in the event of non-attendance or absences.	Statutory processing pursuant to the Education (Welfare) Act 2000. • Attendance records including Registers and Roll books etc. • Records of referrals to TUSLA School Register and Roll Books are documents of enduring historical value and are retained in the school's archives for archival purposes in the public interest.
School tours/trips: Information required to make appropriate travel arrangements, to implement insurance cover, to arrange appropriate supervision ratios, to ensure medical/health issues are properly accommodated, to engage in responsible planning, and to ensure necessary paperwork for INIS (Irish Border Control/Irish Naturalisation & Immigration Service requirements where children are travelling with someone other than their parent or guardian).	Information to ensure trip is properly organised and supervised, including: • permission slips (signed by parents/guardians), • itinerary reports • Letter from parent(s)/guardian(s) giving consent to travel. • Copy of birth/adoption certificate or guardianship papers • Copy of marriage/divorce certificate (where parent has different surname to child). • Copy of the parent/guardian's passport or State identity document.
Garda vetting outcomes: Certain work experience roles may require that a student be Garda vetted (Statutory vetting process).	Information as set down in National Vetting Bureau (Children and Vulnerable Persons) Act 2012. • Garda vetting form

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 (e.g. at front gates, in the car-park etc) and at certain internal points (e.g. 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, • Learning 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 purposes. • Child protection records • Child safeguarding records • Other records relating to child welfare • Meitheal meetings convened by TUSLA
Counselling & Pastoral Care Records: This	• Guidance Counselling notes

information is required to provide access to counselling services and/or 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.	• Psychological service notes • Referrals to/records relating to therapeutic services and other interventions • Minutes, notes and other records concerning Student Support Team/Pastoral Care Team Meetings
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)
Financial information, fees etc: Without this information, the school cannot process applications, make grant payments, or receive payment of monies (e.g. course fees, school trips etc). After completion of the payments, the documentation is retained for audit and verification purposes. The school's financial data are audited by external auditors. Relevant financial information such as a fee statement is also passed onto the College's solicitor in the event of non-payment of fees.	• Information relating to payments from student's parents/guardians (including fee support and fee waiver documentation), • Scholarship/Grant applications (including Gaeltacht, book rental scheme etc).
5. Charity Tax Back Forms This information is required so that the school may avail of the scheme of tax relief for donations of	

money received.	
To claim the relief, the donor must complete a certificate and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. This information is retained by the School in the case of audit by the Revenue Commissioners.	• CHY3/CHY4 tax back forms • Donor name, Address & Telephone Number • PPS Number • Tax Rate • Signature • Gross amount of donation
6. Parent Nominees on Boards of Management This information is required to enable the Board of Management to fulfil its statutory obligations.	
Processing undertaken in accordance with the Education Act 1998 and other applicable legislation, including decisions taken for accountability and good corporate governance.	• Name, address and contact details of Parent Nominee • Records in relation to appointment to the Board • Minutes of Board of Management meetings and correspondence to the Board.

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 Post-Primary Online Database (P-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.[10] The DES has published a "Fair Processing Notice" to explain how the personal data of students is processed.[11]

State Examinations Commission (SEC) data on entrants for the state examinations is provided via the October Returns to SEC to assist its planning of the state examinations.

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). Data to support student access to further and higher education may also be shared for processing as part of *Student Universal Support Ireland* (SUSI), *Higher Education Access Route* (HEAR) and *Disability Access Education Route* (DARE).

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.*[12] 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 (auditors, 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 and Universities/Colleges/Institutes where the student transfers to *another educational body*, or goes on an exchange programme or similar, the school may be asked to supply certain information about the student, such as academic record, references, etc.

Work Placement some data may be shared, on request, with work placement providers and *employers* where this is appropriate and necessary to support students engaged in work experience or similar programmes.

---

[10] 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.

[11] These can be found on www.education.ie (search for Circular Letters 0047/2010 and 0023/2016 in the "Circulars" section). 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 & Employment Affairs 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.

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

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.

Service Providers in some circumstances the school has appointed third parties to undertake processing activities on its behalf. These Data Processors have provided guarantees that their processing satisfies the requirements of the General Data Protection Regulation. The school has implemented written contractual agreements with these entities to ensure that the rights of data subjects receive an appropriate level of protection. Third party service providers include the following categories:

- School Management Information Systems (e.g. VSWare/Advanced/Eportal)
- Productivity Applications (e.g. Google Apps for Education, Microsoft 365)
- Online Storage & File Sharing (e.g. Dropbox, Google Drive, iCloud, OneDrive)
- Video Sharing and Blogging Platforms (e.g. Youtube, Wordpress)
- Virtual Learning Environments (e.g. Edmodo, Schoology, Schoolwise, Google Classroom)
- IT Systems Support (local ICT Support Company)
- Fee management software
- School communications
- Security and CCTV Systems
- Pension Consultants/Trustees
- Accounting & Payroll software
- Cashless Payment Systems (Easypay)
- Catering Management System
- Learning software and Apps

Transfers Abroad In the event that personal data may be transferred outside the European Economic Area (EEA) the school will ensure that any such transfer, and any subsequent processing, is carried out in strict compliance with recognised safeguards or derogations (i.e., those approved by the Irish Data Protection Commission).

Appendix 4. 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.[13]

(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) CCTV[14] (ii) Data Breaches (iii) Data Access Requests (iv) Record Storage and Retention (v) Data Processing Agreements.[15]

(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.[16]

(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 installation of an

[13] The GDPR4schools.ie website identifies some of the GDPR Roles and Responsibilities held by different groups, namely (i) Board of Management (ii) Headmistress/Head Headmistress (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.

[14] A template CCTV policy for Schools is available from www.dataprotectionschools.ie .

[15] 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 Protection Procedures (iii) Code of Behaviour (iv) Guidance and Counselling (v) Policy on Special Education Needs (vi) Anti-Bullying Policy.

[16] 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.

extensive CCTV system in a school is an example of a processing activity that might trigger the need for a Data Protection Impact Assessment.) 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 staff, establishment of password policies, protocols around device encryption, procedures governing access to special category data etc.

(viii) Data Protection by Design The school aims to apply the highest standards in terms of its approach to data protection. For example, school staff will utilise a *Privacy by Design* approach when any activity that requires the processing of personal data is being planned or reviewed. This may mean implementing technical measures (e.g. security) and organisational measures (e.g. protocols and training).

(ix) Data Protection by Default A *Privacy by Default* approach means that minimal processing of personal data is the school's default position. In practice this means that only essential data will be collected from data subjects, and that within the school, access to this data will be carefully controlled and only provided to employees where this is appropriate and necessary.

(x) Data Processing Agreements: the school will put written contracts in place with organisations that process data on its behalf (as required under GDPR Article 28). [17]

(xi) Data Breach Records: the school will retain records that document its handling of any personal data breaches. These records will clearly set out the facts relating to any personal data breach, its effects and the remedial action taken. [18]

(xii) Staff Awareness and Training All who are granted access to personal data that is under the control of the school have a duty to observe the data processing principles. The school will provide appropriate information, training and support so that staff may gain a clear understanding of these requirements.[19]

2. Lawful Processing

As part of its decision to collect, use or share personal data, the school as Controller will identify which of the lawful bases is applicable to each processing operation. In the absence of a lawful basis the personal data cannot be processed.

(i) Many of school's data processing activities rely on legal obligations. These tasks are undertaken because the school must comply with Irish (or European) law[20]. For example, there is a legislative basis underpinning the sharing of specific student data with the Department of Education and Skills and other public bodies.

(ii) Another set of data processing activities are undertaken in the public interest i.e. so that the school can operate safely and effectively. For example, an educational profile of the student

[17] A Data Processing Agreement may be provided as a set of agreed clauses or as an addendum to a broader *(Third Party) Service Agreement*.

[18] These record-keeping requirements are detailed under GDPR Article 33(5). Documentation need to be retained in school setting out details of all data breaches that have occurred. This includes those that were adjudged not to require notification to the Data Protection Commission (in addition to data breaches that required formal DPC notification via https://forms.dataprotection.ie/report-a-breach-of-personal-data).

[19] All current and former employees of the school may be held accountable in relation to data processed by them during the performance of their duties. For example, employees acting in breach of the Data Protection Act 2018 could, in certain circumstances, be found to have committed a criminal offence.

[20] For example, the *Education Act 1998*, the *Education (Welfare) Act 2000* & the *Education for Persons with Special Education Needs Act 2004*.

(literacy competence, language spoken at home etc.) may help the school to target learning resources effectively for the benefit of the student.

(iii) In some situations, for example the use of CCTV, the school may rely on its legitimate interests to justify processing. In such cases the specific legitimate interests (e.g. health and safety, crime prevention, protection of school property etc.) must be identified and notified to the data subjects[21].

(iv) Contract will provide a lawful basis for some processing of data by the school. For example, the processing of some employee data may rely on this lawful basis.

(v) There is also the possibility that processing can be justified in some circumstances to protect the Vital Interests of a data subject, or another person. For example, sharing some data subject data with emergency services might rely on this lawful basis.

(vi) Finally there is the option of using a data subject's consent as the lawful basis for processing personal data. The school will not rely on consent as the basis for processing personal data if another lawful condition is more appropriate. Consent will usually be the lawful basis used by the school to legitimise the publication of student photographs in print publications and electronic media.

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.[22] Some of these processing conditions, those most relevant in the school context, are noted here.

[21] Data subjects have a right to object to processing that is undertaken based on legitimate interests. In such cases the Controller must demonstrate that there is an overriding need if the processing is to continue.

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

(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.

(iii) Processing is based on Explicit Consent. Where a school is processing biometric data for identification purposes (e.g. facial image recognition or the use of fingerprint systems) it is unlikely that this processing will be justifiable on any lawful basis other than consent. (And, as a data subject should be able to withhold consent without suffering any detriment, the school will need to provide access to an alternative processing option which is not reliant on biometric data.)

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.[23]

(i) Transparency is usually achieved by providing the data subject with a written document known as a *Privacy Notice* or a *Privacy Statement*.[24] 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);
- the rights of the data subject. [25]

(ii) Transparency information should be provided in a manner that is concise and easy to understand. To best achieve this, the school may use a "layering" strategy to communicate information.[26] And, while a written *Privacy Notice* is the default mode, transparency information may also be communicated using other means, for example through the spoken word or through use of pictorial icons or video.

(iii) Privacy statements (include those used on school websites) should be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data.

---

[23] GDPR Articles 13 (or 14)

[24] 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.

[25] In the interests of transparency, the school should ensure that its preferred route for a rights request is identified clearly in *Privacy Notices* and elsewhere e.g. *"A data subject wishing to make an access request should apply in writing to the Headmistress."* Notwithstanding this, school staff should be made aware that valid requests may be submitted in a variety of formats (i.e. not necessarily in writing).

[26] For example, where the first point of contact is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13 by way of further, different means, such as by sending a copy of the privacy policy by email and/or sending the data subject a link to the controller's layered online privacy statement/notice.

6. Purpose Limitation

(i) Personal data stored by the school has been provided by data subjects for a specified purpose or purposes.[27] Data must not be processed for any purpose that is incompatible with the original purpose or purposes.[28]

(ii) Retaining certain data (originally collected or created for a different purpose) with a view to adding to a school archive for public interest, scientific or historical research purposes or statistical purposes is acceptable subject to certain safeguards, most particularly the need to respect the privacy of the data subjects concerned.

7. Data Minimisation

As Controller, the school must ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In practice, this principle has a number of important implications illustrated in the examples below.

(i) The school should ensure, when data is being collected from data subjects, that this is limited to what is necessary for the completion of the duties. For example, where information is being collecting from students and parents/guardians, as part of the admissions process, this should be limited to whatever information is needed to operate the admissions process. This means that it is usually not appropriate for the school to seek information about Special Education Needs (SEN) in order to decide whether a place should be offered.[29]

(ii) Data minimisation also requires that the sharing of student data within the school should be carefully controlled. Members of staff may require varying levels of access to student data and reports. Access should be restricted to those who have a defined processing purpose. Staff will not access personal data unless processing is essential to deliver on their role within the school.

(iii) School staff will necessarily create personal data in the course of their duties. However employees should ensure that this processing is necessary and appropriate. For example, while it will often be necessary for school staff to communicate information to each other by email, consideration should be given, on a case-by-case basis, as to whether it is necessary for personal data to be included in these communications.

(iv) Data sharing with external recipients should be continuously reviewed to ensure it is limited to that which is absolute necessary. This may mean, for example, that when the school is seeking professional advice, no personal data will be included in communications unless the disclosure of this information is essential.

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.

---

[27] This purpose is usually communicated to data subjects at the time of collection through providing them with a *Privacy Notice*.

[28] Data Protection Commission: *Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data. You should ask yourself whether the data subject would be surprised to learn that a particular use of or disclosure of their data is taking place.*

[29] SEN data may be sought where the processing of such data is necessary as part of the Admissions Policy. For example, SEN data may be required to consider whether the student fulfils the criteria for admission to a special education needs unit within a mainstream school.

(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[30]).

(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.[31]

(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.

(vi) The important contribution that organisational policies can make to better compliance with the Accountability principle was previously highlighted. Similarly, the implementation of

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

[31] 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).

agreed policies and protocols around data security is very helpful. Some possible areas are listed below.

- School ICT policy
- Acceptable User Polices for employees, board members, students etc
- Accessing school data from home
- Password policy
- Use of staff personal devices in school
- Use of school devices outside school
- Bring Your Own Device Policy
- Social Media Policy
- Mobile phone code
- School use of Apps and Cloud Based Systems

Appendix 5. 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.[32]

(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).[33]

(iii) If requests are manifestly unfounded or excessive[34], 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[35]). 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[36] 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.[37]

(vii) The school must be conscious of the restrictions that apply to rights requests.[38] Where unsure as to what information to disclose, the school reserves the right to seek legal advice.[39]

(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.

---

[32] 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.

[33] 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.

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

[35] 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.

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

[37] 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.

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

[39] 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.

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.

(iii) Where a request relates to video, then the school may offer to provide the materials in the form of a series of still images. If other people's images cannot be obscured, then it may not prove possible to provide access to the personal data.[40]

[40] Where an image is of such poor quality that it does not relate to an identifiable individual, then it may not be considered to be personal data.

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

DES Data Protection Page https://www.education.ie/en/The-Department/Data-Protection/Information.html

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/