Document name	RETNS Policy on Data Protection
Version reference & date of effect	Current version & date of effect: 2.1 - 24 February 2025 Previous versions & dates of effect: 2.0 - 07 December 2020
Document owner	Board of Management
Approved by	Board of Management
Ratified on	24 February 2025
Next Review Date (To be reviewed annually)	2028

Table of Contents

Introduction:

The RETNS Data Protection Policy applies to the processing of personal data held by the school which is protected by the Data Protection Acts 1988 -2018. This policy was first developed in 2017, reviewed in 2020 and will be reviewed periodically to incorporate any changes as to how RETNS treats data that it collects and relevant legislative changes.

Policy Statement:

The Data Protection Acts 1988 -2018 apply to the keeping and processing of personal data, both in manual and electronic form. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to school staff, and to inform staff, pupils and their parents/guardians how their data will be treated.

Relationship to characteristic spirit of school:

Rathfarnham Educate Together National School seeks to

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

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

Scope:

The policy applies to all school staff, the Board of Management, parents/guardians, pupils (past and present) and others, including but not limited to prospective or potential pupils and their parents/guardians and applicants for staff positions within the school, in so far as the measures under the policy relate to them and in so far as the school handles or processes their personal data in the course of their dealings with the school.

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

1 Data Protection Principles

The school is a data controller of personal data relating to its past, present and future staff, pupils, parents/guardians and other members of the school community. As such, the school is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 -2018. The legislative framework can be summarised as follows:

- General Data Protection Regulation (GDPR) 2018
- Data Protection Act 2018
- the "Law Enforcement Directive" (Directive (EU) 2016/680) which has been transposed into Irish law by way of the Data Protection Act 2018
- the Data Protection Acts 1988 and 2003

The principles of data protection may be summarised as follows:

1.1 Obtain and process personal data fairly, lawfully, and transparently:

Information on pupils is gathered with the help of parents/guardians and staff. Information is also transferred from pupils' previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the school, parents/guardians of pupils, etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the school. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained lawfully and processed fairly. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

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

Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. However, further processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes (in accordance with Article 89(1) GDPR) is not considered to be incompatible with the initial purposes.

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

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

Data relating to individuals will only be processed in a manner consistent with the purposes for

which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

1.4 Keep personal data safe and secure:

Only those with a genuine reason for doing so may gain access to information. Sensitive personal data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Personal data stored on portable devices such as laptops, are encrypted and password protected before the devices are removed from the school premises.

Confidential information is stored securely, and, in relevant circumstances, will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

During a period of home working, the school principal and secretary can access their school desktops using 2-factor authentication.

1.5 Keep personal data accurate, complete and up to date:

The school will send an annual form requesting data updates to parents. Pupils, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up to date. Once informed, the school will make all necessary changes to the relevant records. The Principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration to be made to any original record/documentation should be dated and signed by the person making that change. The annual form will also request permission to publish photos of the pupils and their work on the school website.

1.6 Ensure that it is adequate, relevant and not excessive:

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

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

Generally, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage and retention of personal data and sensitive personal data relating to a pupil. Data retention timeframes relating to a pupil, as set out in the Data Retention Schedules, will be followed. The Data Retention Schedules are available on request from the school office.

In the case of members of staff, the school will comply with both DES guidelines and the

requirements of the Revenue Commissioners regarding the retention of employee records. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and/or defending a claim under employment legislation and/or contract and/or civil law.

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

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

2 Lawful Basis for Processing Personal Data

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.

When processing **special category personal data**, the school will ensure that it has additionally identified an appropriate lawful basis under GDPR Article 9. 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.

3 Rationale

In addition to its legal obligations under the broad remit of educational legislation, RETNS has a legal responsibility to comply with the Data Protection Acts, 1988 -2018.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As more and more data are generated electronically, and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognized that recording information accurately and storing it safely facilitates evaluation of the information when necessary, enabling the Principal and Board of Management to make decisions in respect of the efficient running of the school. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and Board of Management.

4 Related Documentation - Other Legal Obligations

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

- Under section 9(g) of the Education Act 1998, the parents of a pupil, or a pupil who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education.
- Under section 20 of the Education (Welfare) Act 2000, the school must maintain a register of all pupils attending the school.
- Under section 20(5) of the Education (Welfare) Act 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring.
- Under section 21 of the Education (Welfare) Act 2000, the school must record the attendance or non-attendance of pupils registered at the school on each school day.
- Under section 28 of the Education (Welfare) Act 2000, the school may supply personal data kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the school is satisfied that it will be used for a "relevant purpose", which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training.
- Under section 14 of the Education for Persons with Special Educational Needs Act 2004, the school is required to furnish to the National Council for Special Education, and its employees, which would include Special Educational Needs Organisers, SENOs, such information as the council may from time to time reasonably request.
- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act, such as the Department of Education and Skills, etc., these records could be disclosed if a request is made to that body.
- Under section 26(4) of the Health Act 1947, a school shall cause all reasonable facilities, including facilities for obtaining names and addresses of pupils attending the school, to be given to a health authority who has served a notice on it of medical inspection, for example, a dental inspection.
- Under Children First: National Guidance for the Protection and Welfare of Children 2011, published by the Department of Children and Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to Tusla - the Child and Family Agency, or in the event of an emergency and the unavailability of Tusla, to An Garda Síochána.
- Certain pupil data may be shared with the HSE for the purpose of the School Health Programme. The legal basis for this is; articles 6 and 9 of the General Data Protection Regulations; Infectious Diseases (Amendment) (No. 2) Regulations 2024; Health (Provision of Information for Health Examination and Treatment Service) Regulations 2024.

5 Personal Data:

Storage of Personal Data

Personal data is stored in secure, locked filing cabinets or electronic databases that only personnel who are authorised to use the data can access. Electronic records are stored with appropriate password protection, with appropriate electronic security measures in place.

Employees are required to maintain the confidentiality of any data to which they have access.

- The personal data records held by the school are set out in the appendices which includes details of both storage and retention limits. The personal data records **may** include:

A Staff records:

i. **Categories of staff data**: As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:
   - Name, address and contact details, PPS number
   - Original records of application and appointment to promotion posts
   - Details of approved absences (career breaks, parental leave, study leave, etc.) Details of work record (qualifications, classes taught, subjects, etc.)
   - Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
   - Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES child protection procedures)
   - Details of complaints and/or grievances including consultations or competency discussions, action/improvement/evaluation plans and record of progress.

ii. **Purposes**: The purposes of keeping staff records are:
   - the management and administration of school business (now and in the future)
   - to facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
   - to facilitate pension payments in the future
   - human resources management
   - recording promotions made (documentation relating to promotions applied for) and changes in responsibilities, etc.
   - to enable the school to comply with its obligations as an employer, including the preservation of a safe, efficient working and teaching environment; and including complying with its responsibilities under the Safety, Health and Welfare at Work Act 2005
   - to enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, Tusla, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies

- for compliance with legislation relevant to the school.

B- Pupil records:

I. **Categories of pupil data**: These may include information which may be sought and recorded at enrolment and may be collated and compiled during the course of the pupil's time in the school. These records may include:

- name, address and contact details
- PPS number
- date and place of birth
- names (including birth surnames) and addresses of parents/guardians and their contact details , including any
  special arrangements with regard to guardianship, custody or access
- whether English is the pupil's first language and/or whether the pupil requires English language support
- any relevant special conditions, for example, special educational needs, health issues, etc., which may apply
- information on previous academic record, including reports, references, assessments and other records from any previous school(s) attended by the pupil
- psychological, psychiatric and/or medical assessments
- attendance records
- photographs and recorded images of pupils, including at school events and noting achievements
- records of significant achievements
- whether the student is exempt from studying Irish
- records of disciplinary issues/investigations and/or sanctions imposed
- records of any serious injuries/accidents, etc. (It is advisable to inform parents that a particular incident is being recorded.)
- records of any reports the school (or its employees) have made in respect of the pupil to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines, subject to the DES child protection procedures.

ii. **Purposes**: The purposes for keeping pupil records are:

- to enable each pupil to develop to their full potential
- to comply with legislative or administrative requirements
- to ensure that eligible pupils can benefit from the relevant additional teaching or financial supports
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents/guardians of their child's educational progress or to inform parents of school events, etc.
- to meet the educational, social, physical and emotional requirements of the pupil
- photographs and recorded images of pupils are taken to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school
- to ensure that the pupil meets the school's admission criteria
- to ensure that pupils meet the minimum age requirements for their class
- to ensure that any pupil seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/ information about the student to the Department

of Education and Skills, the National Council for Special Education, Tusla, and other schools, etc., in compliance with law and directions issued by government departments
- to furnish, when requested by the pupil (or their parents/guardians in the case of a pupil under 18 years) documentation/information/ references to second level educational institutions.

C -Board of Management records:

i. **Categories of Board of Management data:**

These may include:
- Name, address and contact details of each member of the Board of Management, including former members of the Board of Management
- Records in relation to appointments to the board
- Minutes of Board of Management meetings and correspondence to the board which may include references to particular individuals.

ii. **Purpose:** To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.

D -*Other records*
Some **examples** of the type of other records which the school will hold are set out below:

Creditors:

I. **Categories of data:** the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):
- name
- address
- contact details
- PPS number
- tax details
- bank details
- amount paid

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

Charity tax-back form:

i. **Categories of data**: the school may hold the following data in relation to donors who have made charitable donations to the school:
- Name
- Address
- Email address

- Telephone number
- PPS number
- Tax rate
- Signature
- Gross amount of donation

ii. **Purpose:** Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY3 or 4) and forward it to the school to allow it to claim the grossed-up amount of tax associated with the donation. The certificate is retained by the school in the case of audit by the Revenue Commissioners.

CCTV Images/Recordings:

CCTV is in operation at RETNS to monitor the external boundaries of the school, that is, perimeter walls/fencing and internal areas as detailed in the school's CCTV Policy.
These CCTV systems may record images of staff, students and members of the public who visit the premises.

i. **Purpose**: Safety and security of staff, pupils and visitors and to safeguard school property and equipment.

ii. **Location**: Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is in the reception office of school.

iii. **Security**: Access to images/recordings is restricted to the Principal, Deputy Principal and School Secretary of the school. Hard drive recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988, 2003 and 2018.

Examination Results:

i. **Categories**: The school holds data comprising examination results in respect of its students. These include continuous assessment and class, annual, screening and standardised tests.

ii. **Purpose**: The main purpose for which these results and other records are held is to monitor a pupil's progress and to provide a sound basis for advising them and their parents/guardians about their progress. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

6 Recipients

Recipients 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 C). This list may be subject to change from time to time.

6.1 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.
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.

7 Personal Data Breaches

7.1 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.

7.2 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.

7.3 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.

8 Data Subject Rights

8.1 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

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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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.

8.8 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.

8.9 Right not to be subject to automated decision making

This right applies in specific circumstances (as set out in GDPR Article 22).

8.10 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.

8.11 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.

8.12 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 Principal who is responsible for operational oversight of this policy.
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

9 Dealing with Data Access Requests

9.1 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.

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).

iii. If requests are manifestly unfounded or excessive, 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). 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 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.

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

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.

9.2 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.

9.3 Providing information over the telephone:

In RETNS, any employee dealing with telephone enquiries should exercise caution about disclosing any personal information held by the school over the phone. In particular the employee should:

i. Check the identity of the caller to ensure that information is only given to a person who is entitled to that information

ii. Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified

iii. Refer the request to the principal for assistance in difficult situations.

10 Data Protection Issues during Periods of School Closure

10.1 Communication during Periods of School Closure

- Particular attention should be paid to email correspondence
- Subject lines should contain nothing personal or confidential
- Multiple copies of emails should be sent using 'bcc'
- Always check email is sent to intended recipient
- Correspondence to children is sent using parents' email addresses only

10.2 Distance Learning

Children's work is stored electronically on teachers' laptops or on teachers' Google Drive. Staff devices are password–protected.

In circumstances where teaching cannot be conducted on the school premises, teachers and ANAs, acting under the direction of teachers, may use a range of online platforms including Google Classroom, Google Meet, Zoom, Seesaw, Padlet, Skype, Microsoft Teams, Class Dojo and other

platforms approved by the principal to assist with distance teaching and learning. Parental permission is received prior to using any of these platforms.

The school has signed up to the terms of service of the online platforms in use by the school.
The school has enabled the most up to date security and privacy features which these online platforms provide.
Staff members adhere to school guidelines on the use of platforms for live engagement.

10.3 Data protection pertaining to website:

See ICT Acceptable Usage Policy, including section on Distance Learning.

11 Links to other Policies, Guidelines and Protocols

Relevant school policies already in place or being developed or reviewed shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed. The following policies may be among those considered:

- Child Safeguarding Statement and Risk Assessment
- Anti-Bullying Policy
- Code of Behaviour
- Admission Policy
- CCTV Policy
- ICT Acceptable Use Policy

12 Implementation Arrangements, Roles and Responsibilities

In RETNS, the Board of Management is the data controller and the Principal is assigned the role of coordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to personal data are familiar with their data protection responsibilities.

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

Name	**Responsibility**
Board of Management:	Data controller
Principal:	Implementation of policy
Teaching staff:	Awareness of responsibilities
Administrative staff:	Security, confidentiality
ICT personnel:	Security, encryption, confidentiality

13 Ratification and Communication

When the Data Protection Policy has been ratified by the Board of Management, it becomes the school's agreed Data Protection Policy. The entire staff must be familiar with the Data Protection Policy

and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on pupils, staff and others in the school community.

Parents/guardians and pupils should be informed of the Data Protection Policy from the time of enrolment of the pupil, for example, by including the Data Protection Policy as part of the enrolment pack, or by enclosing it or incorporating it as an appendix to the enrolment form.

14 Monitoring and Policy Implementation

The implementation of the policy shall be monitored by the Principal and a sub-committee of the Board of Management.

A note as part of a Report to the School Community will be issued by the Board of Management at least once a year to confirm that the actions/measures set down under the policy are being implemented.

15 Review and Policy Evaluation

The policy shall be reviewed and evaluated at certain times and as necessary. Ongoing review and evaluation shall take cognisance of changing information or guidelines, for example, from the Data Protection Commissioner, Department of Education and Skills or the NEWB, legislation and feedback from parents/guardians, pupils, school staff and others. The policy shall be revised as necessary following such reviews / evaluation and, also, within the framework of school planning.

Contact details:

The Principal
RETNS
Loreto Avenue Rathfarnham Dublin 14 Telephone:
(01)493 8677
E-mail: info@retns.ie

Appendices:

2 Appendix A: Additional Data Protection Schedule For RETNS
3 Appendix B: Glossary
4 Appendix C: Implementing the Data Processing Principles
5 Appendix D: Categories of Recipients
6 Appendix E; Reference Sites
7 Appendix F: RETNS Data Retention Schedule – available on request from school

16 Appendix A: Data Protection (Location and Storage of Records)

Aladdin	Aladdin is the school's official digital depository. A GDPR- compliant data processing agreement with Aladdin has been signed and is available on request. Access to Aladdin is password protected and staff only have access to data which is relevant to their work.	
DATA COLLECTED	**NATURE OF DATA**	**STORAGE/ACCESS**
SECTION 1	**DATA AND THE SCHOOL OFFICE**	
Pupil enrolment information	This includes name, address, date of birth, PPS number, details of parents/ guardians – home address, email address, phone number, medical information, religion, ethnicity	Enrolment form – completed online Aladdin (permissions set for access to data) Personal data collected and stored on Aladdin in order to pass on to government agencies for inclusion on POD encrypted, Hard copy on pupil's file Archived material in strong room Aladdin Medical information shared with school staff when necessary and with medical personnel in emergency

		situation. Could be shared with NCSE with permission of parents
Standardised test results		Aladdin Shared with parents and with DES in 2nd, 4th & 6th
Updating Contacts and Permissions Form	The data here is submitted on an annual basis to the school for the purposes of safety re dropping to and collecting from school, access to children by parents/guardians and nominated others, and updates parents/guardians permissions for various school protocols (trips) and medical-updates.	This data is retained for the full duration of the child's time in school. It is collected using Google forms/ Aladdin Connect and is shared with principal, secretary and class teacher. This information is kept indefinitely.
Financial Information	Account files Bank statements	Electronic files (access is password protected) and hard copies Paper copies – stored in locked cabinet
Service Providers: repairs, builders, maintenance contractors, tradespeople	Names, addresses, phone numbers, email addresses	Electronic database – shared with principal Kept on file for future use
School supplies, company representatives	Names, addresses, phone numbers, email addresses	Locked cabinet Shared with staff

Data Processor e.g. school admin software, school accounting, school photographer	Names, addresses, phone numbers, email addresses	Electronic and / or hard copy files Shared with principal Kept as long as data is processed on behalf of BoM
Emergency services – Garda (including Community Garda), fire brigade	Phone numbers of local services	Shared with principal and staff

SECTION 2	**DATA AND THE PRINCIPAL**	
Teacher / employee data	The school holds teacher, ANA and all employee data in hardcopy-files. Data for teachers and ANAs is also inputted into the OLCS system. The data collected are all necessary for the governance of the school in keeping with BOM governance protocols. These include: • Name, address and contact details, PPS number, Teaching Council number • Next of kin contact name and phone number • Original records of application, contracts and appointment to promotion posts • Garda vetting • Details of approved absences (career breaks, maternity leave, parental leave, study leave, unpaid leave etc.) • Details of work record (qualifications, classes taught, subjects, etc.) • Details of sick leave • Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties – recorded at time of accident • Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES child protection procedures) • Details of complaints and/or grievances including consultations or competency discussions, action/improvement/evaluation plans and record of progress • Details of promotions • Seniority list	The hardcopy files are kept in a locked cabinet in the principal's office. Only personnel who are authorized to use the data can access the data. Employees are required to maintain the confidentiality of any data to which they have access. Some information is held on electronic file Shared with DES and BoM Information on accidents may be shared with medical personnel, school insurers, HSA

	On a voluntary basis staff members may also provide their bank details (for the purposes of remuneration and refund of expenses)	
	The Principal and Deputy Principal are authorised approvers of all school data held on the DES's OLCS system	This access is password protected for Principal and Deputy Principal as approvers, and for the secretary as data- inputter.
Pupil Data	Pupils' psychological and other assessments – occupational therapist, speech and language therapist, psychiatrist	Locked filing cabinet, copy kept in locked filing cabinet in SEN coordinator's room Shared with NCSE, DES with parental permission
	Irish exemptions	Locked filing cabinet
	Legal / custody orders	Locked filing cabinet
	Child protection files	Details recorded at time of concern, Locked filing cabinet, identified using code kept in separate locked drawer Shared with Túsla if considered to reach threshold (advice may be sought), Garda in emergency situation, parents/ guardians

	Accident forms	Folder in principal's office – recorded at time of accident by teacher (generally teacher on duty in yard)
	Yard incidents	Recorded in yard book, more serious incidents reported to principal Shared with parents/ guardians and when necessary: medical personnel, insurers, HSA Yearly audit by Health and Safety Officer on Board of Management
	Correspondence and meetings with parents/ guardians	Pupil's file – hard copy and / or electronic file
BoM members	Names, email addresses	Electronic file Shared with: Patron, Charities Regulator, DES

SECTION 3	DATA AND TEACHERS	
		Each teaching room has a secure lockable cabinet for the purposes of storing sensitive data Psychological, psychiatric and/or educational assessments are kept in individual files in a locked cabinet in Room 3 (SEN coordinator's room) and in the Principal's office. Access is restricted to staff working with a particular child. Assessments and other sensitive information may not be removed from the school building but should be studied on-site.
Teachers and Aladdin	Teachers' records; Pupil progress report card, attendance, relevant medical information and standardised test scores on Aladdin. SETs record IEPs on Aladdin	Aladdin - Teachers should not divulge their Aladdin password to any other person, and passwords should not be stored by default on the class computer. Aladdin should be closed down when not in use. Hard copies of school reports are also stored in the child's individual file in the locked filing cabinet and archived under the stairs when the child leaves the school. Shared with parents Data such as standardised test results shared with school to which pupils transfer

		Data can be shared with NCSE and DES with parental permission Roll books are no longer used but used roll books kept in strong room
Teacher Generated Documents	Any documentation generated by a teacher, or shared with the teacher by a parent / guardian, that refers to issues of a medical nature or school attendance should be kept on the child's file in a locked filing cabinet. Reports concerning child protection concerns remain in principal's office	Relevant documentation is accessed by staff as necessary. Children's files are archived in a locked cupboard under the stairs when the child leaves the school.
Correspondence between teachers and parents/ guardians on educational matters	Pupil file – locked cabinet in teacher's room	Shared with principal and BoM when deemed necessary – kept until issue is dealt with
Record of complaints made by parents / guardians		Locked cabinet in classroom, shared with principal when deemed necessary and kept in locked cabinet in principal's office Shared with BoM, school insurers and legal advisor when deemed necessary
Pupils' Support Plans	Produced by support teacher in collaboration with parents and class teacher	Recorded on Aladdin – hard copies in pupil's file in support teaching coordinator's room
Medical Files	Medical Files are kept in the child's individual file in the classroom. They are also, where necessary to ensure a child's health and safety, kept in a folder in the staffroom and principal's office. A medical overview with brief details are	Relevant documentation is accessed by staff, as necessary. Sensitive information may not be removed from the school building but should be studied on-

	included in the yard notebook. There is a red folder with full medical details in each teacher's desk drawer and a list of allergies (without names) stuck to the teacher's desk to ensure substitute/new staff will be informed of pupils with medical conditions.	site. Archived material is locked under the stairs.
Teachers' Class notes	Throughout the year the teacher may keep a journal of incidents reflections, and observations as an aide memoire. Initials should be used when referring to a child. Should any of these memoires warrant any further attention under the school's child-safeguarding, anti-bullying or disciple procedure these matters should be brought to the Principal's attention who will then keep a formal record.	Yard Books are stored under the stairs.
Teaching/Learning data and ICT	When the teacher is setting up ICT programmes (e.g. reading eggs/matific) she/he should establish a coded or school-generated identity that will be deleted and disposed of once the programme has been completed. Teachers shall ensure not to cause or facilitate the children in inputting any data to third-party sources that are personal or identifying.	
Website and social media	No personal data of any child in the school community ever to be shared or posted - SEE AUP	

SECTION 4	DATA AND ANAs	
	ANAs keep a journal for recording of incidents, observations and reflections but these entries are understood as aide memoires. Any important or ongoing concern recorded in this aide memoire should be brought to the principal for formal discussion and recording. The ANA's journal should be stored securely and handed to the Principal at the end of the school year and archived securely and indefinitely under the stairs.	Formal records in journals or on school templates or NCSE templates recorded by the ANA are handed to the school Principal at the end of the year for storing and archiving These records are kept indefinitely.

SECTION 5	DATA AND BOARD OF MANAGEMENT	
The BOM is responsible for compliance with the GDPR and Data Protection Acts. The school is not required to appoint a data protection officer, but the BOM authorises the principal to function as an informal DPO while the BOM maintains the governance liability	**The BOM documents are stored securely. Hard copies of the minutes are stored in a locked cabinet.** **Minutes, agendas and other documentation are shared via SLACK**	**Location**: Manual records are stored in a secure, locked filing cabinet in the Principal's Office. Only personnel who are authorized to use the data can access it. Employees are required to maintain the confidentiality of any data to which they have access. Electronic records (SLACK) are stored with appropriate password protection, with appropriate electronic security measures in place. Older minutes are stored in a locked storage room. These minutes are kept indefinitely.

BOM confidentiality	All BOM members are obliged to observe confidentiality about matters discussed at BOM, and any documents distributed as part of BOM discussions are returned at the end of the meeting and shredded. One copy of all BOM documents will be stored securely.	The principal stores the BOM Minutes in the locked filing cabinet in the locked office. Older minutes are stored in a locked storage room. These minutes are kept indefinitely.
Staff Training	The BOM authorises the principal to direct all staff to undergo training and briefings on data protection on an ongoing basis, and breaches of GDPR will be dealt with under the school's Complaint and Grievance procedure	
Financial records	The financial records of the school are treated as confidential and are only disclosed to the school's authorised accountant.	**Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access. Annual audited accounts to be kept indefinitely

SECTION 6	DATA AND OTHER AGENCIES	
Tusla and Tusla authorised services, Garda, Revenue Commissioners, Department of Social Protection, Applications on foot of court order	The school will comply fully with all authorised and lawful requests from these statutory agencies	**All correspondence relating to these matters will remain in a locked cabinet in the Principal's Office** **Emails of a confidential nature are printed and kept in a locked cabinet**
Family Solicitors	Requests for school data from a family solicitor, whether via a parent/guardian, or independently delivered to the school, will be dealt with on a case by case basis and may require legal advice or consultation with the National Data Protection Office.	**All correspondence relating to these matters will remain in a locked cabinet in the Principal's Office**
Research Projects, Public Relation Exercises, Student teachers/TY and ANA students	The principal, in consultation with the Board when deemed necessary, will on an ongoing basis approve research projects, public relations exercises and access to the school by student-teachers, TY and ANA students etc. which are deemed to be of benefit to the school community. The principal will inform the parents/guardians of such placements.	When engaging in these projects, the principal will ensure the highest ethical standards apply and that there is no potential harm and indeed a particular educational gain for the school community.
HSE and private health professionals	Any data requested by a health professional can only be released with the explicit permission of the child's parent. The school keeps a record of any such shared data in a locked cabinet in the principal's office.	
Community Organisations	Community organisation may not collect data from children on their visits to the school, nor will the school facilitate the sharing of any such data.	
Department of Education and Skills and DES officers	The DES is the Data Protection controller of the POD and OLCS systems, and are responsible for any breaches of this data. The school complies with any sharing of data to the Inspectorate that may arise during school evaluation (e.g. access to IEPs, teacher-folders, anti-bullying data, child safeguarding data etc.)	

17 Appendix B: 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 (but does not include 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.

18 APPENDIX C: 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.[1]

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 (ii) Data Breaches (iii) Data Access Requests (iv) Record Storage and Retention (v) Data Processing Agreements.[2]

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):

1. the purposes of the processing;
2. a description of the categories of data subjects and personal data;
3. the categories of recipients to whom the personal data will be disclosed;
4. any transfers to a third country or international organisation, including suitable safeguards;
5. where possible, the envisaged time limits for erasure of the different categories of data;
6. 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.[3]

[1] 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.

[2] 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.

[3] 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

ii. 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 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.

iii. 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.

iv. 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).

v. 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.

vi. 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). [4]

vii. 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. [5]

---

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.

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

[5] 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).

viii. 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.[6]

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[7]. 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 (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[8].

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.

[6] 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.

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

[8] 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.

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.[9] 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.

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

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.[10]

i. Transparency is usually achieved by providing the data subject with a written document known as a *Privacy Notice* or a *Privacy Statement*.[11] 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. [12]

[10] GDPR Articles 13 (or 14)

[11] 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.

[12] 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 Principal."* 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).

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.[13] 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.

6. Purpose Limitation

i. Personal data stored by the school has been provided by data subjects for a specified purpose or purposes.[14] Data must not be processed for any purpose that is incompatible with the original purpose or purposes.[15]

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.[16]

[13] 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.

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

[15] 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.*

[16] 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.

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.

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[17]).

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.

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

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.[18]

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 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

[18] 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).

- 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
- Apps

19 APPENDIX D: 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. The DES has published a "Fair Processing Notice" to explain how the personal data of students is processed.

Health Service Executive (HSE) Certain pupil data may be shared with the HSE for the purpose of the School Health Programme.

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.* 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 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.

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)
- 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 (x)
- School communications (x)
- Security and CCTV Systems (x)
- Pension Consultants/Trustees (x)
- Accounting & Payroll software (x)
- Cashless Payment Systems (x)
- Canteen Management System (x)
- Learning software and Apps (x)

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).

20 Appendix E: 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/