Data Protection Policy

Introductory Statement

We have had data protection legislation in Ireland since 1988 and have taken data protection compliance seriously and are already in good shape for meeting General DataPersonal Regulation (GDPR) increased compliance standards. GDPR builds upon and enhances, many of the existing data protection requirements and principles under current Irish data protection legislation.

From 25 May 2018, GDPR will replace the 1995 Data Protection Directive, which is the EU legislation on which the main Irish data protection legislation, the Data Protection Acts 1988 and 2003 (as amended) (DPA), is based. There will also be Irish implementing national legislation to give further effect to and provide for exemptions from, GDPR. In Ireland, the Department of Justice and Equality published the General Scheme of the Data Protection Bill 2017 in May 2017 (General Scheme). The General Scheme essentially sets out the heads that are proposed to be included in the Irish implementing legislation when it is enacted.

The school's Data Protection Policy applies to the personal data held by the school's Board of Management (BoM), which is protected by the Data Protection Acts 1988 to 2018 and the EU GDPR. This policy replaces the school's original Data Protection Policy, which has been in place since 2007. The policy applies to all school staff, the Board of Management, parents/guardians, pupils, and others (including prospective or potential pupils and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and special categories of personal data will be protected by the school.

Privacy

Dunboyne Junior Primary School operates a "Privacy by Design" method in relation to Data Protection. The GDPR contains the new concepts of privacy by design and by default, intended to strengthen the protection of privacy by requiring organisations to build consideration of privacy into their product and service design processes in certain cases. The GDPR, unlike the Directive, also requires formal Data Protection Impact Assessments in relation to higher-risk processing activities.

Privacy by design

Privacy by design requires data controllers to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to apply the data protection principles effectively and to integrate the necessary safeguards into the processing to meet the requirements of the GDPR and protect the rights of data subjects. In ascertaining the appropriate technical and organisational measures required to be implemented the controller is required to have regard to the following:

- The cost of implementation

• The nature, scope, context and purposes of processing

• The risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing

A. Privacy by default

Privacy by default requires data controllers to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing are processed. The privacy by default obligation applies to:

1. The amount of personal data collected
2. The extent of the processing
3. The period of storage, and
4. The accessibility of the data Compliance with the requirements of privacy by default and design may be demonstrated by an approved certification mechanism.

This means in Dunboyne Junior Primary School we plan carefully when gathering personal data so that we build in the data protection principles as integral elements of all data operations in advance. We audit the personal data we hold in order to:

- be able to provide access to individuals to their data
- ensure it is held securely
- document our data protection procedures
- enhance accountability and transparency

Data Protection Principles

The school BoM 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 BoM is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 to 2018 and GDPR, which can be summarised as follows:

1. Obtain and process Personal Data fairly

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

2. Consent

Where consent is the basis for provision of personal data, (e.g. data required to join sports team/ after-school activity or any other optional school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes. Dunboyne Junior Primary School will require a clear, affirmative action e.g. ticking of a box/signing a document to indicate consent. Consent can be withdrawn by data subjects in these situations.

Valid consent

A lawful basis is required for the processing of personal data. The grounds for lawful processing in the GDPR replicate those in the Directive. One of the lawful grounds for processing is the

consent of the data subject. The GDPR tightens the concept of consent. Accordingly, obtaining the consent of a data subject will be more difficult under the GDPR. In particular, this is due to the requirement of separate consents for different processing operations, the prohibition on including consent in the terms of service, and the data subject's express right to withdraw his or her consent at any time.
Under the GDPR, in order to provide a lawful basis for processing, the consent of a data subject must be:
1. Freely given – Consent will not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.
2. Specific – When the processing has multiple purposes, consent should be obtained for each of them.
3. Informed – For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data is intended. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
4. An unambiguous indication of the data subject's wishes by a statement or clear affirmative action – Clear affirmative actions which may provide evidence of consent include ticking a box when on a webpage, choosing technical settings on a website, or any other statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes or inactivity will not suffice. In order for consent to be valid, four additional criteria must be complied with:

1. **Onus of proof**: The controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data. Consequently, a record should be maintained evidencing a data subject's consent.

2. **Independent consent clauses**: Where consent is provided in a written declaration, such as a contract, that contains additional matters, the request for consent must be clearly distinguishable from other matters in that declaration. It must further be intelligible, easily accessible and be in clear and plain language. A consent clause contained in the middle of a set of general terms and conditions is unlikely to suffice.

3**. Right of withdrawal**: The data subject is entitled to withdraw his or her consent at any time and must be informed of the existence of this right. It must be as easy to withdraw as it is to give consent.

4. **Voluntary**: When assessing whether consent is freely given, utmost account must be taken of whether the performance of a contract is conditional on a data subject consenting to the processing of personal data that is not necessary for the performance of that contract. Consent in such instances is unlikely to be regarded as freely given. There is no change in the law in respect of the requirement of explicit consent for the processing of sensitive data. Similar to the Directive, no definition of explicit consent is provided in the GDPR. In some instances it may be permissible to rely on existing consents secured under the Directive. It is not necessary for the data subject to give his or her consent again if the way the consent given under the Directive is in line with the conditions of the GDPR. In such cases, the data controller may continue processing on the basis of consent given prior to the date the GDPR takes force. However, in many cases, historic consents may not be compliant with the requirements of the GDPR. Data controllers will accordingly need to review historic consents to determine their compliance with the GDPR.

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

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

4. 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

5. Keep Personal Data safe and secure

Only those with a genuine reason for doing so may gain access to the information. Personal Data is securely stored under lock and key in the case of manual records and protected with computer software and password protection in the case of electronically stored data. (Aladdin, our Student Management System is GDPR compliant.) Portable devices storing personal data (such as laptops) are encrypted and password-protected.

6. Keep Personal Data accurate, complete and up-to-date

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. Records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/documentation should be dated and signed by the person making that change

7. 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

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

As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of Personal Data relating to a student. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law. See School Record Retention table Appendix 1.

9. Provide a copy of their personal data to any individual on request

Individuals have a right to know and have access to a copy of personal data held about them, by whom, and the purpose for which it is held.

Scope

The Data Protection legislation applies to the keeping and processing of *Personal Data*. 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
The policy applies to all school staff, the Board of Management, parents/guardians, pupils and others (including prospective or potential pupils and their parents/guardians, and applicants for

staff positions within the school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

Definition of Data Protection Terms

In order to properly understand the school's obligations, there are some key terms, which should be understood by all relevant school staff:
Personal Data means any data relating to an identified or identifiable natural person i.e. a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller (BoM)
Data Controller is the Board of Management of the school.
Data Subject is an individual who is the subject of personal data.
Data Processing performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data
- Retrieving, consulting or using the data
- Disclosing the data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blocking, erasing or destroying the data

Data Processor a person who processes personal information on behalf of a data controller, but **does not include an employee of a data controller** who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection legislation places responsibilities on such entities in relation to their processing of the data. The school uses a number of services where student and staff data is collected: Aladdin (staff and pupils), School Accounting (for staff), Blacknight (web hosting).

Special categories of Personal Data refers to *Personal Data* regarding a person's:

- racial or ethnic origin
- political opinions or religious or philosophical beliefs
- physical or mental health
- sexual life and sexual orientation
- genetic and biometric data
- criminal convictions or the alleged commission of an offence
- trade union membership

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. This means any compromise or loss of personal data, no matter how or where it occurs

Rationale

In addition to its legal obligations under the broad remit of educational legislation, the school has a legal responsibility to comply with the Data Protection Acts 1988 to 2018 and the GDPR. 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. The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the Principal and Board of Management to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to

ensure that there is consistency and continuity where there are changes of personnel within the school and Board of Management.

Other Legal Obligations

Implementation of this policy takes into account the school's other legal obligations and responsibilities. Some of these are directly relevant to data protection. For example:
Under **Section 9(g) of the Education Act, 1998**, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in their education.
Under **Section 20 of the Education (Welfare) Act, 2000**, the school must maintain a register of all 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. Dunboyne Junior Primary School sends, by post or email, a copy of a child's reports and assessment, to the Principal of the School in which the pupil has been enrolled.
Where reports on pupils which have been completed by professionals, apart from Dunboyne Junior Primary School staff, are included in current pupil files, such reports are only passed to the other school following express written permission having been sought and received from the parents of the said pupils.
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, Tusla, the National Council for Special Education and other schools). The BoM must be 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; 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) 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 most schools are not currently subject to freedom of information legislation, (with the exception of schools under the direction of Education and Training Boards), if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education, etc.) these records could be disclosed by that body if a request is made to that body.
Under **Section 26(4) of the Health Act, 1947** a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection.
Under **Children First Act 2015**, mandated persons in schools have responsibilities to report child welfare concerns to TUSLA- Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationship to characteristic spirit of the School:

Dunboyne Junior Primary School seeks to:
enable pupils 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. The school wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection legislation.

Personal Data
The *Personal Data* records held by the school **may** include:

1. Staff records:

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.
- Name and contact details of next-of-kin in case of emergency.
- 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 Children First Act 2015.

Purposes: Staff records are kept for the purposes of:

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

Location and Security procedures of Dunboyne Junior Primary School:

1. Manual records are kept in a secure, locked filing cabinet in a locked administration office only accessible to personnel who are authorised to use the data. Employees are required to maintain the confidentiality of any data to which they have access.
2. Digital records are stored on password-protected computer with adequate encryption and firewall software in a locked office. The school has the burglar alarm activated during out-of-school hours.

2. Student records:

The GDPR introduces a number of specific requirements relating to the processing of children's data.

- Online consents
- Where information society services, such as online services, are offered directly to a child under the age of 16 and the child is required to consent to the processing of his or her personal data, parental consent must be obtained. However, the controller is required to make 'reasonable efforts' to verify that consent has been given or authorised by the parent/guardian of the child, bearing in mind available technology. This means specific verification measures should be used.
- Specific protections must be applied to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.
- The introduction of this age limit will not affect contract law rules on the validity, formation or effect of a contract in relation to a child.

Privacy notices

- Controllers are required to take appropriate steps to ensure that the provision of information to data subjects is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is especially important in respect of information addressed specifically to a child. Where processing is addressed to a child, any information and communication should be in such a clear and plain language that the child can easily understand.

Legitimate interests

- The pursuit of legitimate interests by the controller or a third party is a basis for lawful processing instead of consent. Relying on this basis involves a balancing test between the competing interests involved. The interests of the controller or third party may be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. The protection of a child's interests as a data subject is particularly important.

Categories of student data:

These may include:

- Information, which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
- name, address and contact details, PPS number
- date and place of birth
- names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
- religious belief
- racial or ethnic origin
- membership of the Traveller community, where relevant
- whether they (or their parents) are medical card holders
- whether English is the student's first language and/or whether the student requires English language support
- any relevant special conditions which may apply
- Information on previous academic record
- Psychological, psychiatric and/or medical assessments
- Attendance records

- Photographs and recorded images of pupils (including at school events and noting achievements) are managed in line with the accompanying policy on school photography.
- Academic record – as recorded on official School reports
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Other records e.g. records of any serious injuries/accidents
- Records of any reports the school (or its employees) have made in respect of the student to State Departments and/or other agencies under Children First Act 2015
- Purposes: The purposes for keeping student records include:
- to enable each student to develop to his/her 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 support the provision of religious instruction
- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events, etc.
- to meet the educational, social, physical and emotional requirements of the pupil
- photographs and recorded images of pupils are taken to celebrate school achievements, e.g. compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the School Website Privacy Statement. See Appendix 4
- to ensure that the student meets the school's admission criteria
- to ensure that pupils meet the minimum age requirement for attendance at Primary School.
- 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, the National Council for Special Education, TUSLA, and other schools, etc. in compliance with law and directions issued by government departments

Board of Management records:

- Categories of Board of Management data:
- 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 individuals.
- Purposes:
- To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of Board appointments and decisions.
- (Location and Security procedures as above):

Other Records: Creditors

Categories of Board of Management data:

- The school may hold some or all of the following information about creditors (some of whom are self-employed individuals):
- name
- address
- contact details
- PPS number

- tax details
- bank details and
- amount paid

Purposes: The purposes for keeping creditor records are:

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. (Location and Security procedures as above):

Other Records: Charity Tax-back Forms

Categories of Board of Management data:

The school may hold the following data in relation to donors who have made charitable donations to the school:

- name
- address
- telephone number
- PPS number
- tax rate
- signature and
- the gross amount of the donation.

Purposes: The purposes for keeping creditor records are:

Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents' name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the event of audit by the Revenue Commissioners. (Location and Security procedures as above):

Examination results

The school will hold data comprising examination results in respect of its pupils. These may include class, mid-term, annual and continuous assessment results and the results of Standardised Tests.

Purposes:

The main purpose for which these examination results are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardian about educational attainment levels and recommendations for the future. 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, the National Council for Curriculum and Assessment and other schools to which pupils move. Location and Security procedures are as outlined above.

Links to other policies and to curriculum delivery

Our school policies need to be consistent with one another, within the framework of the overall School Plan. 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:

- Pupil Online Database (POD): Collection of the data for the purposes of complying with the Department of Education' pupil online database.
- Safeguarding Children
- Anti-Bullying Procedures
- Code of Behaviour
- Admissions Policy
- ICT Acceptable Usage Policy
- Assessment Policy
- Special Educational Needs Policy
- Critical Incident Policy
- Attendance Policy / Attendance Strategy

Processing in line with a data subject's rights

Data in this school will be processed in line with the data subject's rights. Data subjects have a right to:

- Know what personal data the school is keeping on them
- Request access to any data held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended
- Ask to have data erased once it is no longer necessary or irrelevant.

Data Processors

Where the school outsources to a data processor off-site, it is required by law to have a written contract in place (Written Third party service agreement See Appendix 2). Dunboyne Junior Primary School's third party agreement specifies the conditions under which the data may be processed, the security conditions attaching to the processing of the data and that the data must be deleted or returned upon completion or termination of the contract.

Personal Data Breaches

All incidents in which personal data has been put at risk must be reported to the Office of the Data Protection Commissioner within 72 hours. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the BoM must communicate the personal data breach to the data subject without undue delay. If a data processor becomes aware of a personal data breach, it must bring this to the attention of the data controller (BoM) without undue delay.

Dealing with a data access request

Individuals are entitled to a copy of their personal data on written request. The individual is entitled to a copy of their personal data. Request must be responded to within one month. An extension may be required e.g. over holiday periods. Data can only be guaranteed to be recovered during term time. Requests can be made from September 1st to June 30th each year. Any request outside of this time will not be guaranteed their data within one month of the request. No fee may be charged except in exceptional circumstances where the requests are repetitive or manifestly unfounded or excessive. No personal data can be supplied relating to another individual apart from the data subject. Any Data Subject about whom the school holds personal data has a right to find out, free of charge, if a person (an individual or an organisation) holds information about him/her. The Data Subject also has a right to be given a description of the information and to be told the

purpose(s) for holding the information. Applications for the release of data should always be in writing (rather than over the phone) and should state the purpose for which it is required. See Appendix 2. Data protection legislation allows exemptions in relation to schools providing, or 'disclosing', information to:

- The Gardaí
- The Revenue Commissioners
- Department of Social Protection (DSP)
- Applications on foot of a court order
- Tusla (Child and Family Agency). See Appendix 3.

Providing information over the phone

An employee dealing with telephone enquiries should be careful about disclosing any personal information held by the school over the phone. In particular, the employee should:

- Ask that the caller put their request in writing
- Refer the request to the In School Management Team / Principal for assistance in difficult situations
- Not feel forced into disclosing personal information

Implementation arrangements, roles and responsibilities

The BoM is the data controller and the Principal implements the Data Protection Policy, 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

Ratification & communication

Ratified at the BoM meeting on June 19th, 2018 and signed by Chairperson. Secretary recorded the ratification in the Minutes of the meeting.

Monitoring the implementation of the policy

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

Reviewing and evaluating the policy

The policy will be reviewed and evaluated after two years. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education or TUSLA), legislation and feedback from parents/guardians, pupils, school staff and others. The policy will be revised as necessary in the light of such review and evaluation and within the framework of school planning.

Appendix 1: DATA RETENTION PERIODS

Pupil Related	**Retention Periods**
School Register/Roll Books	Indefinitely
Enrolment Forms	Hold until Pupil is 25 Years
Disciplinary notes	Never Destroy
Test Results – Standardised	Hold until pupil is 25 Years
Psychological Assessments etc.	Never Destroy
SEN Files/IEPS	Never Destroy
Accident Reports	Never Destroy
Child Protection Reports/Records	Never Destroy
S.29 Appeals	Never Destroy
Interview Records	
Interview Board Marking Scheme Board of Management notes (for unsuccessful candidates)	18 months from close of competition plus 6 months in case Equality Tribunal needs to inform school that a claim is being taken
Staff Records	
Contract of Employment Teaching Council Registration Vetting Records Accident/Injury at work Reports	Retention for duration of employment + 7 years (6 years to make a claim against the school plus 1 year for proceedings to be served on school)
BoM Records	
BOM Agenda and Minutes CC TV Recordings (if any, none currently) Payroll & Taxation Invoices/receipts Audited Accounts	Indefinitely 28 days normally. In the event of criminal investigation – as long as is necessary Revenue require a 6-year period after the end of the tax year Retain for 7 Years Indefinitely
Why, in certain circumstances, does the Data Protection Commission recommend the holding of records until the former pupil has attained 25 years of age? The reasoning is that a pupil reaches the age of majority at 18 years and that there should be a 6-year limitation period in which it would be possible to take a claim against a school, plus 1 year for proceedings to be served on a school. The Statute of Limitations imposes a limit on a right of action so that after a prescribed period any action can be time barred.	

Appendix 2: Request for a copy of Personal Data under the Data Protection Acts 1988 to 2018

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

Full Name:	
Maiden Name *(if name used during* your school duration*)*	
Address:	
Contact number *	Email addresses *

* We may need to contact you to discuss your access request

Please tick the box, which applies to you:

Parent/Guardian of current Pupil ☐	**Former Pupil** ☐	**Current Staff Member** ☐	**Former Staff Member** ☐
Name of Pupil:		Date of Birth:	
Insert Year of leaving:		Insert Years From/To:	

DATA ACCESS REQUEST:

I, …… [name] wish to make an Access Request for a copy of personal data that Dunboyne Junior Primary School holds about me/my child. I am making this access request under Data Protection Acts 2013 to 2018. To help us to locate your personal data, please provide details below, which will assist us to meet your requirements e.g. description of the category of data you seek. Any other information relevant to your access request (as otherwise it may be very difficult or impossible for the school to locate the data)

I declare that all the details I have given in this form are true and complete to the best of my knowledge.

Signature of Applicant ……. Date: …….

Appendix 3: Written Third Party service Agreement.

In accordance with the Data Protection Acts 1988 to 2018 and General Data Protection Regulation (GDPR), the Board of Management of Dunboyne Junior Primary School requires this written third party service agreement to be in place with all our data processors. GDPR requires that the Board of Management shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of GDPR and thus ensure the protection of the rights of the data subject.

The Board of Management of Dunboyne Junior Primary School as data controller imposes the following minimum obligations on you as data processor:

1. To act only on the documented instructions of the data controller i.e. the Board of Management of **Dunboyne Junior Primary School with regard to the subject-matter, the types of personal data processed, the documented purposes of the processing and the duration of the processing**.
2. To comply with the obligations imposed on data controllers by the Data Protection Acts 1988 to 2018 and GDPR in order to ensure that appropriate steps are taken to ensure the confidentiality of the personal data being processed and to guard against the accidental destruction, damage or loss of personal data.
3. To provide sufficient guarantees in respect of technical security measures and organisational measures governing the processing of the school's data.
4. To provides an indemnity to the school board of management for any breaches of the above legal conditions.
5. To commit to the provision of assistance where appropriate to enable the school board to comply with a data subject access request.
6. To immediately contact the school principal Orla Mahon, where there are any data security breaches in the data processor's company to in order to facilitate the school board as data controller to take the required action in accordance with the GDPR regarding the data breach.
7. To comply with the requirements of the Data Protection Policy of Dunboyne Junior Primary School.
8. On termination of the contract between the data processor and the Board of Management of Dunboyne Junior Primary School, all personal data held by the data processor must be returned to the Board as data controller or in the alternative, it must be entirely deleted from the data processor's systems and files.
9. To make available to the controller (B.O.M.) all information necessary to demonstrate compliance with the obligations of the GDPR and to allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
10. If the processor believes that any instruction it receives from the controller is in breach of the GDPR, the processor shall immediately inform the controller.

(*This agreement should be signed by the Data Processor and the Board of Management of the school and copies retained by both).*

Dunboyne Junior Primary School, Station Road, Dunboyne, Co. Meath or by email to **office@dunboynejps.ie**