Data Protection Policy

Reviewed
April 2020

Ennis National School

Index

1.Definitions used in this policy

i. **Ennis National School, Us, We, Our**
    a. Ennis National School, Us, We & Our all refer to Ennis National School Limited located at Ennis NS, Ashline, Kilrush Road, Ennis, Co Clare, V95 DE44 with registered number :

ii. **You**
    a. You refers to all individuals, organisations and third parties that we require to comply with this policy

iii. **Students, Parents and Guardians**
    a. **Students, Parents and Guardians** includes all individuals and organisations currently, historically or prospectively engaging in our services, including website visitors.

iv. **Services**
    a. Our services include but are not limited to:
        i. providing education services to our students

ii. providing extra curricular activities to our students
iii. providing employment to our Teachers, Special Needs Assistants and Ancillary Staff

v. Data Protection Representative

a. We have appointed the following individual / organisation to handle all our data protection related queries: Brian Troy Principal.

vi. Criminal records
For the purposes of this policy criminal records data means data about an individual's criminal convictions and offences, and data relating to criminal allegations and proceedings.

vii. **Data protection laws**
For the purposes of this policy Data Protection laws means all applicable laws relating to the processing of Personal Data, including, for the period during which it is in force, the General Data Protection Regulation (Regulation (EU) 2016/679).

viii. **Data Subject**
Data subject means the individual to whom the personal data relates.

ix. **Personal Data**
Personal data means any data that relates to an individual who can be identified from that data

x. **Processing**
Processing means any use that is made of data, including but not limited to collecting, storing, amending, disclosing, or destroying it.

xi. **Special categories**
Special categories of personal data means data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

.

1(a). Legal Obligations

1. Implementation of this policy takes into account the school's other legal obligations and responsibilities. Some of these are directly relevant to data protection.
2. 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.
3. Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School
4. 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.
5. Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day.

6. 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 and 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 educational 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).
7. 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.
8. 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.
9. 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 or immunization administration.
10. Under Children First: National Guidance for the Protection and Welfare of Children (2017), schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána) and to maintain documentation according to the highest confidentiality standards.

2. Statement and purpose of policy

i. Ennis National School is committed to ensuring that all personal data handled by us, will be processed according to legally compliant standards of Data Protection.

ii. We confirm for the purposes of the data protection laws, that Ennis National School may be a data controller of your personal data and the personal data of our Students, Parents and Guardians. This means that we determine the purposes for which, and the manner in which your personal data and our Students, Parents and Guardians personal data is processed.

iii. The purpose of this policy is to help us achieve our Data Protection aims by:

a. notifying you of the types of personal data that we may hold about you and our Students, Parents and Guardians, and what we do with that data;
b. setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, transfer, store or otherwise process personal data and ensuring you understand our rules and our legal standards;
c. clarifying your responsibilities and duties in respect of Data Protection.

iv. This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

3.Data protection principles

i. When your work involves processing personal data relating to other Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members members, our Students, Parents and Guardians, or any other Data Subjects, you must comply with this policy and with the following data protection principles which require that personal data is:

a. Processed lawfully, fairly and in a transparent manner.
    i. We must always have a lawful basis to process personal data, as set out in the data protection laws.
    ii. Personal data may be processed as necessary
        1. To deliver services to the data subject,
        2. To comply with a legal obligation which the data controller is the subject of,
        3. Or for the legitimate interests of the data controller or the party to whom the data is disclosed.
        4. The data subject must be told
            a. who controls the data (us),
            b. the purpose(s) for which we are processing the data and
            c. to whom it may be disclosed.

b. Collected only for specified, explicit and legitimate purposes.
    i. Personal data must not be collected for one purpose and then used for another.
    ii. If we want to change the way we use personal data, we must first tell the data subject.
c. Processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
d. We will only collect personal data to the extent required for the specific purpose notified to the data subject.
accurate.
    i. Ennis National School takes all reasonable steps to ensure that data that is inaccurate is rectified or deleted without delay.
    ii. Checks to personal data will be made when collected and regular checks must be made afterwards.

iii. We will make reasonable efforts to rectify or erase inaccurate data.

e. Kept only for the period necessary for processing.
   i. data will not be kept longer than it is needed and we will take all reasonable steps to delete data when we no longer need it.

f. Secure, and appropriate measures are adopted by Ennis National School to ensure as such.

4.Who is responsible for Data Protection?

i. Maintaining appropriate standards of Data Protection is a collective task shared between us and you.

ii. This policy and the rules contained in it apply to all Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and any other individual or organisation carrying out the processing of Personal data on behalf of Ennis National School, irrespective of seniority, tenure and working hours.

iii. Questions about this policy, or requests for further data, should be directed to the Data Protection Representative.

iv. All Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members have a personal responsibility to ensure compliance with this policy,
   - To handle personal data consistently with the principles set out here and to ensure that measures are taken to protect the data security.
   - Those in management positions have special responsibility for leading by example and monitoring and enforcing compliance.
   - The Data Protection Representative must be notified if this policy has not been followed, or if it is suspected that this policy has not been followed, as soon as reasonably practicable.

v. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal.

vi. Significant or deliberate breaches, such as accessing Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members or Students, Parents and Guardians personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

vii. **The role of the Data Protection Representative is :**

viii. To advise Ennis National School and its Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members what their responsibilities are under the GDPR and the Data Protection Acts.
ix. To monitor compliance with the GDPR and the Data Protection Acts and relevant policies.
x. To provide training and carry out awareness to Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and keep a record of such training.
xi. To provide guidance on the completion of Data Protection Impact Assessments.
xii. To co-operate and act as the contact point with the Data Protection Commission in relation to complaints, investigations, audits and consultations and any other matter relevant to the legislation.

Contact details for the Data Protection Representative is: Brian Troy, Principal, Email: principal@ennisns.ie Tel: 065 6829158

5.What personal data and activities are covered by this policy?

1. This policy covers personal data:
    a. Which relates to any natural living individual who can be identified either from that data in isolation or by reading it together with other data we possess;
    b. Is stored digitally or physically;
    c. In the form of statements of opinion as well as facts;
    d. Which relates to Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members (present, past or future) or to any other individual or organisation whose personal data we handle or control;
    e. Which relates to Students, Parents and Guardians (present, past or future) or to any other individual or organisation whose personal data we handle or control;
    f. Which we obtain, is provided to us, which we hold or store, organise, disclose or transfer, amend, retrieve, use, handle, transport, destroy or otherwise process.
    g. This personal data is subject to the legal safeguards set out in the relevant data protection laws.

6. What personal data do we process?

i. We process personal data about our Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members, Students, Parents and Guardians and others which:

a. Are provided or we gather before or during your employment or engagement with us;
b. Is provided by third parties, such as references or data from suppliers or another party that we do business with; or
c. Is in the public domain.
d. The types of personal data that we may collect, store and use about our Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and Students, Parents and Guardians include but are not limited to records relating to:

i. **Data we may process about Teachers, Special Needs Assistants, Ancillary Staff, Board of Management :**
    1. Name, address and contact details, PPS number;
    2. Original records of application and appointment to promotion posts;
    3. Details of approved absences (career breaks, parental leave, study leave etc.);
    4. Details of work record (qualifications, classes taught, subjects etc.);
    5. Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties; and
    6. 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).
    7. Garda Vetting related Information

ii. **Data we may process about Students, Parents and Guardians:**
    1. name, address and contact details, including PPS number; date and place of birth;
    2. names and addresses of parents/guardians and their contact details (including any special
    3. arrangements with regard to guardianship, custody or access);
    4. names and details for emergency contacts;
    5. religious belief (with the option of parents to not consent);
    6. racial or ethnic origin (with the option of parents to not consent);
    7. membership of the Traveller community, where relevant (with the option of parents to not consent);
    8. whether they (or their parents) are medical card holders;
    9. whether English is the student's first language and/or whether the student requires English
    10. language support; and
    11. any relevant special conditions (e.g. special educational needs, health issues, etc.) which may apply.
    12. Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student

13. Psychological, psychiatric and/or medical assessments
14. Attendance records
15. Photographs and recorded images of students
16. Academic record – class assignments, standardized test results, school reports
17. Records of significant achievements
18. Whether the student is exempt from studying Irish
19. Records of disciplinary issues/investigations and/or sanctions imposed
20. Other records e.g. records of any serious injuries/accidents
21. Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures)
22. Name, address and contact details, PPS number;
23. Legal Custody status and details;
24. Parents Association related data;
25. Teachers notes relating to Parent Teacher meetings;
26. Parent / Guardian Occupation;

e. We may process other data required by us to provide our Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members with employment and our Students, Parents and Guardians with our Services.

7. Special category data

i. We may from time to time need to process special category personal data (sometimes referred to as 'sensitive data').
   a. This type of data includes
      i. Race and ethnic origin
      ii. Religious or philosophical beliefs
      iii. Political opinions
      iv. Trade union memberships
      v. Biometric data used to identify an individual
      vi. Genetic data
      vii. Health data
      viii. Data related to sexual preferences, sex life, and/or sexual orientation

ii. We will only process special category personal data if:

   a. We have a lawful basis for doing so;

      and

b. One of the following special conditions for processing personal data applies:

i. The data subject has given explicit consent.
ii. The processing is necessary for the purposes of exercising the employment law rights or obligations of the organisation or the data subject.
iii. The processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
iv. Processing relates to personal data which are manifestly made public by the data subject.
v. The processing is necessary for the establishment, exercise, or defence or legal claims; or
vi. The processing is necessary for reasons of substantial public interest.

iii. Before processing any special category personal data, Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members must notify the Data Protection Representative of the proposed processing, in order for the Data Protection Representative to assess whether the processing complies with the criteria noted above.

iv. special category personal data will not be processed until the assessment above has taken place and the individual has been properly informed of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

8. Criminal records data

i. Criminal records data will be processed in accordance with Article 10 of the GDPR which states:
ii. “Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.”

9. How we use your personal data

i. We will tell you the reasons for processing your personal data and our Students, Parents and Guardians personal data, how we use such data and the legal basis for processing in our privacy statement. We will not process your personal data or our Students, Parents and Guardians personal data for any other reason.

ii. In general we will use personal data to carry out our business, deliver our services, to administer employment or engagement and to deal with any problems or concerns data subjects may have, including, but not limited to:

a. *Data Processing Purposes*

10. Accuracy and relevance

i. We will:
   a. Ensure that any personal data processed is up to date, accurate, adequate, relevant and not excessive, given the purpose for which it was collected.
   b. Not process personal data obtained for one purpose for any other purpose, unless you agree to this or reasonably expect this.
   c. If you consider that any data held about you or our Students, Parents and Guardians is inaccurate or out of date, then you should tell the Data Protection Representative. If they agree that the data is inaccurate or out of date, then they will correct it promptly. If they do not agree with the correction, then they will note your comments.

11. Storage and retention

i. Digital Personal data (and special category personal data) will be kept securely in accordance with appropriate Cyber Security standards, such as keeping digital personal data in username and password authenticated systems.
ii. Physical Personal data (and special category personal data) will be kept securely in accordance with appropriate data protection standards such as keeping physical personal data in locked filing cabinets.
iii. The periods for which we hold personal data are contained in our privacy statements.

12.Individual rights

i. All Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and Students, Parents and Guardians have the following rights in relation to their personal data.
   a. Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and Students, Parents and Guardians have the right to be informed about how we process their personal data (Right to be informed)
   b. Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and Students, Parents and Guardians are able to request access to data we hold on them through a Subject Access Request (SAR) (Right of Access); (See Appendix 1)

c. Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and Students, Parents and Guardians can request to change or correct any inaccurate data (Right to Rectification);
d. Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and Students, Parents and Guardians have the right to object to having their data processed (Right to Restriction of Processing);
e. Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and Students, Parents and Guardians can request to delete data that we hold. (Right to Erasure (sometimes referred to as the Right to be Forgotten));
f. Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and Students, Parents and Guardians can request to have their data moved outside of our organisation. (Right to Data Portability);
g. Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and Students, Parents and Guardians can object to a decision made by automated processing, with certain limited exceptions (such as legitimate grounds for the processing or the defence of legal claims) and request that any decision made by automated processes have some human element (Right to Object to Automated Decision Making, including Profiling).

i. To make enquiries, exercise any of your rights set out above, or withdraw your consent to the processing of your Data (where consent is our legal basis for processing your Data), please contact us at Email: principal@ennisns.ie Tel 065 6829158

ii. If you are not satisfied with the way a complaint you make in relation to your Data is handled by us, you may be able to refer your complaint to the relevant data protection authority which in Ireland is the Data Protection Commission www.dataprotection.ie.

iii. It is important that the Data we hold about you is accurate and current. Please keep us informed if your Data changes during the period for which it is held.

13.Data security

i. We will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and

against accidental loss, destruction or damage.

ii. Maintaining data security means making sure that:

a. Only people who are authorised to use the data can access it;
b. Where possible, personal data is pseudonymised or encrypted;
c. data is accurate and suitable for the purpose for which it is processed; and
d. Authorised persons can access data if they need it for authorised purposes.

iii. By law, we must use procedures and technology to secure personal data throughout the period that we hold or control it, from obtaining to destroying the data.

iv. Personal data must not be transferred to any person to process, unless that person has either agreed to comply with our data protection policy, have signed the organisations data processing agreement or we are satisfied that other adequate measures exist.

v. Security procedures include:

a. Any desk or filing cabinet containing personal data must be kept locked.
b. Computers should be locked with a strong password that is changed regularly, or shut down when they are left unattended.
c. Discretion should be used when viewing personal data on a monitor to ensure that it is not visible to others.
d. Data stored on disks, hard drives or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
e. The Data Protection Representative must approve of any cloud used to store data.
f. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
g. All servers containing special category data must be approved and protected by security software.
h. Servers containing personal data must be kept in a secure location, away from general office space.
i. Data should be regularly backed up and those backups should be tested.

vi. Telephone Precautions. Particular care must be taken by Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

a. The identity of any telephone caller must be verified before any personal data is disclosed;
b. If the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;
c. Do not allow callers to bully you into disclosing data. In the event of any problems or uncertainty, contact the Data Protection Representative.

vii. Methods of disposal. Copies of personal data, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper

documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

14. Data impact assessments

Some of the processing that Ennis National School carries out may result in risks to privacy.

Where processing would result in a high risk to Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members or Students, Parents and Guardians rights and freedoms, Ennis National School will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Why do I need to carry out a DPIA?
The purpose of a Data Protection Impact Assessment is to determine if the concept of 'privacy by design' is adequately embedded into processes, systems or projects that will affect or bring about high risk or high-volume processing of personal data.

When do I need to carry out a DPIA?
The list below includes examples of when a DPIA must be carried out however it is not exhaustive.

- If you are working on a research project using a high volume of special category data such as health data or if working with genetic data.
- If you are developing or acquiring a new system than involves processing large volumes of personal data e.g. a new HR database.
- If you are processing a high volume of personal data relating to trade union membership, political opinions, racial or ethnic origin, sexual orientation, etc.
- If you are carrying out a new direct marketing or communications campaign using a database acquired from a third party or a new database compiled from resources such as publicly available personal data.
- If you plan to carry out any type of monitoring or surveillance of individuals including Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members, students and members of the public e.g. CCTV.
- If you plan to use technologies such as biometric or facial recognition for security access systems or otherwise.
- If you are working with new and potentially privacy invasive technology including smart technology, AI and Internet of Things.

15. Data breaches

i. A personal data protection breach ("data breach" in short) usually occurs when:

   a. There is an unauthorised or accidental disclosure of, or access to, personal data.
   b. There is an unauthorised or accidental alteration of personal data.
   c. There is an accidental or unauthorised loss of access to, or destruction of, personal data.
      i. The GDPR defines a data breach 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".

ii. Data breaches may occur in a variety of contexts, such as:

   a. Loss or theft of data (e.g. on a memory stick, laptop or paper records)
   b. Inappropriate access controls (e.g. using insecure passwords)
   c. Equipment failure
   d. Confidential data being left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account, leaving documents on top of shared photocopiers)
      i. Disclosing confidential data to unauthorised individuals
   e. Human error (e.g. emails being sent to the wrong recipient)
   f. Hacking, viruses or other security attacks on IT equipment systems or networks e.g. Ransomware
   g. Breaches of physical security (e.g. forcing of doors/windows/filing cabinets)

iii. If we discover that there has been a breach of Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members or Students, Parents and Guardians personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Data Protection Commissioner within 72 hours of discovery.

iv. We will record all data breaches regardless of their effect in accordance with our Breach response policy.

v. If the breach is likely to result in a high risk to your rights and freedoms, we will inform affected individuals that there has been a breach and provide them with more data about its likely consequences and the mitigation measures that have been taken.

vi. If a data breach has occurred, you will be asked to complete the Data Breach Report Form (See Appendix 2) as soon as possible.

vii. It is much better to report a data protection breach straight away than to "cover it up" and risk negative consequences down the line. A data protection breach is not a

disciplinary issue, and once the breach has been reported the Data Protection Representative will handle things from there.

16. International data transfers

i. In the course of carrying out our business, we may need to transfer Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members or Students, Parents and Guardians personal data to a country outside the European Economic Area (EEA) including to any group company or to another person with whom we have a business relationship.

ii. Personal data will only be transferred to a country outside of the EEA if there are adequate protections in place. To ensure that personal data receives an adequate level of protection, we have put in place appropriate procedures with the third parties we share personal data with to ensure personal data is treated by those third parties in a way that is consistent with and which respects the law on data protection.

17. Individual responsibilities

i. Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members are responsible for helping Ennis National School keep their personal data up to date.

ii. Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members should let Ennis National School know if personal data provided to Ennis National School changes, e.g. if you change address or your bank details.

iii. You may have access to the personal data of other Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and of our Students, Parents and Guardians in the course of your employment where it is business critical to your role. Where this is the case, Ennis National School relies on Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members members to help meet its data protection obligations to Teachers, Special Needs Assistants, Ancillary Staff Members and Board of Management Members and to Students, Parents and Guardians.

iv. Individuals who have access to personal data are required:
    a. To access only personal data that they have authority to access and only for authorised purposes;
    b. Not to disclose personal data except to individuals (whether inside or outside of Ennis National School) who have appropriate authorisation;
    c. To keep personal data secure by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction;

d. Not to remove personal data, or devices containing or that can be used to access personal data, from Ennis National School's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
e. Not to store personal data on local drives or on personal devices that are used for work purposes.

18. Training

i. We will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

ii. A record or training participation and assessment results will be kept by management.

iii. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy will receive additional training to help them understand their duties and how to comply with them.

19. Marketing / Mailing Lists / Electronic Privacy Regulations

i. The Electronic Privacy Regulations 2011 (SI 336 of 2011) sit alongside the Data Protection Acts. They give people specific privacy rights in relation to electronic communications and contain specific rules on:

   a. Marketing calls, emails, texts and faxes
   b. Cookies (and similar technologies)
   c. Keeping communications services secure; and
   d. Customer privacy regarding traffic and location data, itemised billing, line identification, and directory listings.

ii. While primarily aimed at electronic communications companies (telecommunications companies and internet services providers), the Regulations also apply to any entity using such communications and electronic communications networks to communicate with customers, e.g. by telephone, via a website or over email, etc.

iii. Unsolicited direct marketing is one of the main sources of complaint from individuals to the Data Protection Commissioner and anyone who fails to comply with the E-Privacy Regulations can be prosecuted as each unlawful marketing message or call constitutes a separate offence.

iv. It is imperative that the necessary marketing opt-ins and opt-outs (via a data protection notice or otherwise) are in place before using personal data for marketing purposes.

v. Where Ennis National School process personal data to keep people informed about news and offers we must provide in each communication a simple way of opting out of further communications.

Policy Approval

This policy has been reviewed and accepted by the Board of Management of Ennis national School

Chairperson of BOM ……

Date: -