Ard Scoil Ris

Data Protection Policy

Introductory Statement

The school's Data Protection Policy applies to the personal data held by the school which is protected by the Data Protection Acts 1988 and 2003.

The Rationale of the Policy

This policy explains what sort of data is collected, for how long it will be stored and with whom it will be shared. As more and more data is 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 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.

Relationship to School spirit and ethos

Ard Scoil Ris aims to provide a holistic education, which is driven by a Catholic ethos. We strive to create : a safe environment, which fosters inclusion, honesty, dignity and respect; a disciplined environment which allows the teacher to teach and the student to learn. The school community encourages the individual in his pursuit of excellence. We aim to promote among our students a sense of pride in their school. (Our motto : "Dilseacht agus Uaisleacht" encapsulates this).

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, parents/guardians and other 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 Acts.

Links to Other Policies and to Curriculum Delivery

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 Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Admissions/Enrolment Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE/CSPE

Scope of the policy

The policy applies to all school staff, the board of management, parents/guardians, students and others (including prospective or potential students 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 sensitive personal data will be protected by the school.

Purpose of the policy

The Data Protection Acts 1988 and 2003 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 meet its statutory obligations, to explain those obligations to school staff, students and their parents/guardians how their data will be treated.

Definition of Terms

Data Protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data.

Data means information in a form which can be processed. It includes both automated data and manual data. **Automated Data** means any information on computer or information recorded with the intention that it is processed by computer. **Manual Data** means information that is kept/recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. **A relevant filing system** means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to

individuals, so that specific information relating to a particular individual is readily accessible. Examples might include student files stored in alphabetical order in a filing cabinet or personnel files stored in schools or in administrative offices.

Data Controller: Controls the contents and use of data.

Data Processor: Processes data on behalf of data controller.

Processing: Any access to, use or disclosure of personal data. Includes: obtaining, recording, keeping, collecting, organising, storing, altering, adapting, disclosing, aligning, combining, blocking, erasing, or destroying data.

Data Subject: Data relating to identifiable living individuals (not companies or anonymised) In relation to schools, data subjects would include students, employees (teachers, SNAs ancillary staff etc)

Personal Data: Data relating to an individual who can be identified either from the data alone or from the data in conjunction with other information that is in or likely to come into the possession of the data controller. Examples of personal data: student records, photographs, exam results and records, financial information, emails, CCTV images, application forms, CVs and disciplinary reports.

A) Staff Records

Categories of Staff Data including: name, address, contact details, PPS number, original application records, details of approved absences (career breaks, parental leave etc), details of work record (qualifications, classes taught) details of incidents/injuries sustained on school property, disciplinary etc.

Purposes: management and administration of school business. Facilitate payment of staff, entitlements, pension etc. HR management. Record of promotions. Enable school to comply with obligations as an employer etc.

Location: Secure, locked filing cabinet that only authorised personnel have access.

Security: Manual record, computer record or both e.g. locks, padlocks, password protection.

B) Student Records

Categories of Student Data including name, address, contact details, PPS number, place and DOB, religious belief, information on previous academic record, attendance record, medical assessment records.

Purpose: enable student to develop to full potential, comply with legislative requirements, support provision of religious instruction, enable parent/guardian to be contacted in an emergency, meet the student's needs.

Location: Secure filing cabinet.

Security: Manual record, computer record or both e.g. locks, padlocks, password protection.

C) Board of Management

Categories: name, address, contact details, record of appointment, minutes of BOM meetings.

Purpose: operate in accordance with Education Act 1998. Maintain record of board appointments and decisions.

Location: secure, locked filing cabinet where only authorised personnel have access.

Security: Manual record, computer record or both e.g. locks, padlocks, password protection.

D) Other Records

Creditors, charity tax back forms, CCTV recordings and images.

Sensitive Personal Data: Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health and/or details of any criminal allegations, proceedings or convictions.

Data Protection Principles

Given that schools collect, store and process data about living people on computers or in manual format, they are understood to be *data controllers* and have certain key responsibilities in relation to the information held and processed.

These key responsibilities can be summarised in terms of **eight fundamental rules which schools must follow**. These include the obligation to:

Rule 1: Obtain and process information fairly

The data subject must be aware of: -

Data Controller holds personal information about him/her

Purpose for which information kept

Any disclosures of data to third parties

Right to access personal data and have inaccuracies corrected

Data Protection Notice (e.g. terms and conditions, privacy statement, on website)

Rule 2: Keep it only for one or more specified, explicit & lawful purposes

Data is not used for any purpose for which data subject has not been informed

Rule 3: Use and disclose it only in ways compatible with these purposes

Consent will be required where new use of data proposed

Use and disclose data only in ways compatible with purpose

Only collect data which is strictly necessary in relation to the purpose for which it was collected

Rule 4: Keep it safe and secure

Access to data must be on a strict 'need to know' basis

Appropriate measures must be taken against unauthorised access to, alteration, disclosure, destruction or loss of personal data, e.g. appropriate encryption

Duty to ensure staff are aware of and comply with security measures (e.g. checking identity, ensuring legal basis for a request which should be in writing) etc.

Summary -Security Measures: *The school must* -

- Ensure good technical security, e.g. passwords, encryption, firewalls
- Ensure good physical security, e.g. locks, alarms, CCTV
- Ensure high staff awareness
- Ensure confidential disposal of documents e.g. shredding facilities on every floor and boxes for confidential waste which must be brought to a secure location for onward disposal
- Review access to premises or equipment
- Regularly review security arrangements where staff members take personal data off site (e.g. Principal taking files home to work on in spare time) Ensure that the physical files are transported and stored under lock and key and that soft copy files are encrypted and password protected
- Ensure periodic checks are carried out on the school's security measures and that where gaps arise measures are taken to rectify these gaps
- Where data is transferred to a third party processor, ensure that you have written contract in place and a procedure for breach
- Ensure that the school has its own procedure in place for dealing with data breaches

Rule 5: Keep it accurate, complete and up-to-date

Review records periodically to determine what is no longer required and should be destroyed

Establish clear policy on the destruction of records

Ensure records disposed of safely- shredding of paper records, permanently delete data from hard drives and other storage devices

Communicate records management/destruction policy

Provide training appropriate to level of responsibility

Carry out regular audits to ensure policies being followed

Rule 6: Ensure it is adequate, relevant and up to date

The school must:

Identify minimum amount of personal data needed to fulfil the purpose

Ensure the information collected is necessary

There must exist an 'extra' valid reason for asking for sensitive data

Rule 7: Retain it for no longer than is necessary for the purpose or purposes

Data must not be kept for longer than necessary

Data retention may be justified where: required by law; needed to take or defend legal proceedings; other legitimate business reason

Define a retention policy for the school with reference to the nature and format of data being held

Rule 8: Give a copy of their personal data to that individual on request

Furnish copy of his/her personal data to that individual on request

Ratification and Communication

Upon ratification by the Board of Management, the finalised draft becomes the school's agreed Data Protection Policy. It will then be circulated within the school community. 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.

Parents/guardians and students should be informed of the Data Protection Policy from the time of enrolment of the student e.g. by including the Data Protection Policy as part of the Enrolment Pack, by either enclosing it or incorporating it as an appendix to the Enrolment Form.

Monitoring the implementation of the policy

Implementation Date: 3rd May 2017

This policy will be reviewed annually or as need arises, whichever occurs first.