BACKGROUND INFORMATION ON DATA PROTECTION POLICY

1.0 Introduction

1.1 St John the Apostle NS, Knocknacarra has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Dept of Education and Skills, Data Protection Commissioner's Office, other advisory groups and guidance issued by professional bodies.

1.2 The Data Protection Commissioner is responsible for upholding the rights of individuals, as set out in the Acts, and enforcing the obligations upon data controllers. The Commissioner is appointed by Government and is independent in the exercise of his or her functions. Individuals who feel their rights are being infringed can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it.

1.3 Non compliance with the legislation could result in penalties, which are punishable by fines.

1.4 This Data Protection Policy aims to detail how meets its legal obligations concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Acts of 1988 and 2003 that are the key pieces of legislation covering the security and confidentiality of personal information.

1.5 For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. See Appendix 1 for summary of compliance with the Data Protection Act.

2.0 Overview of Legislation

Data Protection Acts 1988 and 2003
These Acts are the key pieces of legislation and are therefore covered in detail.

2.1 These Acts apply to all personally identifiable information held in manual files, computer databases, computer screens and other automated media about pupils and school staff.

2.2 The Acts dictate that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff will be considered a disciplinary offence.

2.3 It also requires the school to register its data holdings with the Office of the Data Protection Commissioner identifying the purposes for holding the data, how it is used and to whom it may be disclosed. The school also has to comply with the principles of good practice.

2.4 All applications/databases are required under law to be registered for Data Protection purposes. Registration will be with the Data Commissioner and will comply with the Data Protection Act.

2.5 Under a provision of the Data Protection Act an individual can request access to their information, regardless of the media on which this information may be held / retained.

3.0 Policy Statement

All staff must comply with the Data Protection Principles

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes

.

3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes

4.0 Responsibility

It is the responsibility of the School Principal to ensure that there is compliance with the Data Protection Rules.

4.1 Line Management:

Each teacher is responsible for:

- Ensuring that personal information kept on pupils is only kept for the lawful and clearly specific purpose/s it was taken.
- Ensuring that personal information is only processed (used) in a manner compatible with the consent given by the parent/guardian
- Ensuring procedures are in place to identify who personal information is being disclosed to, why it is being disclosed and what exactly is being disclosed.
- Ensuring personal information, in their area of responsibility, is secure
- Ensuring that periodic review and / or audit is undertaken in their area, to ensure that personal information is kept up-to-date and is accurate.
- Ensuring that records are reviewed on a regular basis, thus identifying areas where errors are most commonly made.
- Be aware of the different data sets used in classroom and their purpose

Staffs are responsible for:

- Not disclosing personal information, in relation to any child to any other individual who is not entitled by law to receive this information
- Complying with this guideline and all other relevant policies, procedures, regulations and applicable legislation
- Respecting and protecting the privacy and confidentiality of the information they process at all times
- Ensuring personal information is secure when in their possession
- Reporting any data breaches to the Principal
- Attending training provided by the Principal, in respect of Data Protection and information practices

5.0 Protocol for Reporting breaches

If any breaches of information practice or of the regulations in the Data Protection Acts are committed it must be reported to the Data Commissioner's Office immediately.

.

Appendix 1

Compliance with the Principles of the Data Protection Acts

1. Obtain and process information fairly

To **fairly obtain** data, the data subject must, at the time the personal data is being collected, be made aware of:

- the identity of the data controller
- the purpose in collecting the data
- the persons or categories of persons to whom the data may be disclosed
- any other information which is necessary so that processing may be fair

To **fairly process** personal data it must have been fairly obtained and the data subject must have given consent to the processing or the processing must be necessary for one of a number of reasons, including:

- to prevent injury or other damage to the health of a data subject or another person
- to prevent serious loss or damage to property of the data subject or another person
- to protect the vital interests of the data subject or another person where the seeking of the consent of either is likely to result in those interests being damaged
- for the administration of justice
- compliance with a legal obligation, other than that imposed by contract
- for the purpose of obtaining legal advice, or in connection with legal proceedings, or for the purposes of establishing, exercising or defending legal rights
- for medical purposes

Any secondary or future uses of personal information, which are not obvious, should be brought to the attention of the parent when the information is being collected. If, at a later date the personal information is going to be used for a new purpose, further consent must be obtained from the parent. If they refuse permission, then the data cannot be used for that purpose and mechanisms must be put in place to reflect this choice.

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

A data controller may only keep data for a purpose/s that are specific, lawful, clearly stated and the data should only be processed in a manner compatible with the purpose. An individual has a right to question the purpose for which their data is held.

To comply with this rule:

- in general, the persons should know the reasons why their data is being collected and retained
- the purpose for the data collections must be lawful

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

Any use or disclosure must be necessary for the purpose/s or compatible with the purpose/s for which the data is being collected.

Some key tests of compatibility are:

- Is the data used only in ways consistent with the purpose/s for which it was obtained?
- Is the data disclosed only in ways consistent with that purpose/s?

A key exception to these rules arises in section 8 of the Act, where disclosure of the information is required by law. Another exception is where the disclosure is made to the data subject himself/herself with his/her consent.

.

4. Keep it safe and secure

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against its accidental loss or destruction.

High standards of security are essential for all personal information. The nature of security used may take into account what is available, the cost of implementation and the sensitivity of the data in **complete and up-to-date** question.

5. Keep it accurate,

To comply with this rule staff must ensure that clerical and computer procedures are adequate to ensure high levels of data accuracy and that the information is kept up-to-date.

Each Deparment within the HSE must undertake periodic review and / or audit to ensure that personal data is kept up-to-date and is accurate.

6. Ensure that it is adequate, relevant and not excessive

To fulfil this requirement staff must keep only the minimum amount of personal data which is needed to achieve the specified purpose/s. The data must be adequate, relevant, and not be excessive and apply those criteria to each item of information and the purpose/s for which it is held.

Each class teacher must periodically review the information sought by it, to ensure it is adequate, relevant and not excessive. If reasons for collecting certain information are redundant, then the collection of that information must be discontinued immediately.

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

This requirement places a responsibility on staff to be clear about the length of time data will be kept and the reason why it is being retained. Files should be regularly purged in accordance with agreed policy so that personal information is not retained any longer than necessary.

8. Give a copy of personal data to an individual, on request

An individual is entitled to:

- a copy of the data held
- know the purpose/s for processing
- know the identity of those to whom the data is disclosed
- know the source of the data, unless it is contrary to public interest
- know the logic involved in automated decisions
- a copy of any data held in the form of opinions, except where given in confidence

What are parents/pupils rights under the Data Protection Acts

In addition to the rights arising from the obligations imposed on Data Controllers by the Eight Principles of Data Protection, parents and pupils also have the following rights:

Right of rectification or erasure

Parents have the right to have information which is inaccurate rectified, or in some cases have the information erased.

Right to block certain uses

A parent can prevent their personal data from being used for certain purposes, e.g. research.

Right to object

A parent, if they feel that the use of their data involves substantial and unwarranted damage or distress to them, may request a data controller to stop using this personal data, or not to start using the data.

The right does not apply if:

- consent has already been obtained
- the use is necessary for a contractual obligation
- the use is required by law
- the processing is to protect the vital interests of the data subject

.