ippn
Leading and Learning

Tacaíocht, Misneach & Spreagadh
Supporting School Leadership

Getting Data Protection Ready

Resource Bundle

Glossary of Terms

Automated Data	means, broadly speaking, any information on computer, or information recorded with the intention of putting it on computer
BoM	Board of Management
CCTV	Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism
Data	means information in a form which can be processed. It includes both automated data and manual data. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system)
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 organisation to which the data controller outsources work e.g. Aladdin, Databiz. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data
Data Controller	any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. This means any organisation or person holding personal data about any individual e.g. the BoM of a School
Data Protection Officer	the DPO is responsible for ensuring that the Data Controller and Data Processor comply with all relevant Data Protection Legislation and the General Data Protection Regulation (GDPR)
Data Subject	is an individual who is the subject of personal data
Manual Data	means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system

Personal Data	any information relating to an identified or identifiable natural person ("Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This means any compromise or loss of personal data, no matter how or where it occurs
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 is accessible
Special Categories of Data	relates to specific categories of data which are defined as data relating to a person's • racial or ethnic origin • political opinions, religious and philosophical beliefs • physical or mental health • genetic and biometric data • sexual life and sexual orientation • criminal convictions or the alleged commission of an offence • trade union membership A Data Subject has additional rights in relation to the processing of any such data.
Data Protection Acts	The Data Protection Acts 1988 to 2018 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and to individuals who interact with the organisation

In this Resource Bundle

1 Introduction 1
1.1 Bunreacht na hÉireann 1
1.2 Fundamental Rights of the European Union 1
1.3 IPPN 1
2 Data Protection and Schools 2
2.1 Why does Data Protection apply to schools? 2
2.2 What are the 8 Rules of Data Protection? 2
2.3 What is the fundamental principle of Data Processing? 2
2.4 What is the legal framework underpinning Data Protection in Ireland? 3
2.5 What is the (EU) GDPR? 3
2.6 What are the Key Changes? 3
2.7 What is the difference between personal, sensitive and non-sensitive data? 4
2.8 What rights have Data Subjects? 4
2.9 Who is the Data Controller in a School? 4
2.10 What is the role of a Data Protection Officer (DPO)? 4
2.11 Does your school need to appoint a DPO? 5
2.12 Who is (are) the Data Processor(s) in a School? 5
2.13 What is meant by Data Processing? 5
2.14 What is meant by Fair Processing? 5
2.15 What is meant by consent? 6
2.16 How does a School ensure that its data is Accurate? 6
2.17 What about transferring Data to another Primary School or to a Secondary School? 7
2.18 What about transferring Data to a data processing company 7
2.19 Who can request Data from a School? 7
2.20 What practical steps should schools take to ensure compliance with GDPR 8
2.21 What additional wording needs to be added to Enrolment Forms 8
2.22 What access have Data Subjects to notes written by Principals and Teachers? 8
2.23 What if Data is Disclosed Unintentionally or Hacked? 9
2.24 What Support is available to Schools to ensure compliance with their Data Protection obligations? 9
2.25 How long must schools retain data 9
2.26 What about CCTV? 10
2.27 What is a Privacy Impact Statement? 11
2.28 Data Protection Policy 11
2.29 Website Privacy Statement 11
3 Resources Available 12
3.1 Useful Websites: 12

1 INTRODUCTION

"*In God we trust. All others must bring data*."
W. Edwards Deming, Statistician

"Security is always excessive until it's not enough"
Robbie Sinclair, Head of Security, NSW Australia

1.1 BUNREACHT NA HÉIREANN

Article 40.3.1, in relation to the Right to Personal Privacy, states that

"The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizens"

Court Interpretation:

"the right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State" [Hamilton P. in Kennedy v. Ireland [1987] IR 587]

1.2 FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Article 8, in relation to the Protection of Personal Data, states that

a) Everyone has the right to the protection of personal data concerning him or her

b) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

1.3 IPPN

The purpose of this IPPN Resource Bundle is to clearly outline the statutory requirements for schools in relation to Data Protection in light of the European Union General Data Protection Regulation, (GDPR). The GDPR has the force of law and its provisions commence simultaneously throughout the European Union, including Ireland, on 25th May 2018.

2 DATA PROTECTION AND SCHOOLS

On 25th May 2018 the provisions of the GDPR will enhance and reform all existing Irish Data Protection Acts. These provisions enhance the rights of Data Subjects and place certain onuses on Data Processors and Data Controllers.

Schools gather, store and process information about people – school staff members, parents, children, suppliers, etc. - and are therefore subject to the GDPR. The GDPR emphasises transparency, security and accountability by Data Controllers and Data Processors, while at the same time standardising and strengthening the right of European citizens to data privacy.

2.1 WHY DOES DATA PROTECTION APPLY TO SCHOOLS?

Schools hold a vast amount of data on pupils, parents and staff. Schools are obligated to seek, hold and process such information in compliance with Data Protection rules.

2.2 WHAT ARE THE 8 RULES OF DATA PROTECTION?

PAM

- Obtain and process information fairly
- Keep it for one or more specified, explicit and lawful purposes
- Process it only in ways compatible with the purpose for which it was given initially
- Use and disclose it in ways compatible with these purposes
- Keep it safe and secure
- Ensure it is adequate and not excessive
- Retain no longer than necessary
- A copy of the data must be made available to the data subject on request.

2.3 WHAT IS THE FUNDAMENTAL PRINCIPLE OF DATA PROCESSING?

"The data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly"

This is the fundamental principle of data protection – **that it be obtained and processed fairly**. If your organisation wishes to keep personal information about people, then you must collect the information fairly, and you must process (or use) the information fairly.

This provision requires that –

At the time of providing personal information, individuals are made fully aware of:

1. the identity of the persons who are collecting it (though this may often be implied)
2. to what use the information will be put
3. the persons or category of persons to whom the information will be disclosed.

Secondary or future uses, which might not be obvious to individuals, should be brought to their attention at the time of obtaining personal data. Individuals should be given the option of saying whether or not they wish their information to be used in these other ways.

If a data controller has information about people and wishes to use it for a new purpose (which was not disclosed and perhaps not even contemplated at the time the information was collected), he or she is obliged to give an option to individuals to indicate whether or not they wish their information to be used for the new purpose.

These are the ways a data controller achieves transparency and informed consent - the touchstones of fairness in data protection.

2.4 What is the legal framework underpinning data protection in Ireland?

- Data Protection Acts 1998 to 2018
- EU Data Protection Directive 95/46/EC
- EU GDPR 2018

2.5 What is the (EU) GDPR?

The new (**European Union) General Data Protection Regulation** (GDPR) gives data subjects the right to request from schools whatever data is being stored about them and to withdraw consent to its use, effectively ordering its destruction. According to Article 12, this request must be free of charge, easy to make, and must be fulfilled within one month. However, a school is entitled to hold lawfully-obtained data about pupils in order for it to carry out its business. As emails can and often do contain personal data, the GDPR requires that schools manage backup and archive copies of them with sufficient rigour.

An additional challenge for schools will be to comply with record retention requirements and respond to an individual's deletion request without the risk of losing others' emails. Schools should have a Data Protection Policy in compliance with the GDPR. Some schools may find it prudent to retain emails for as short a retention duration as possible in order to minimise administration of data access requests.

2.6 What are the key changes?

- Increased sanctions, administrative fines and right to compensation for the individual
- Increased obligations of transparency according to data protection principles
- Record-keeping in relation to the processing of data
- Stricter rules around the obtaining of consent and on relying on consent as a legal basis for data processing
- Appointing an independent Data Protection Officer (DPO)
- Notification of data breaches to the Data Protection Commissioner
- Enhanced rights for data subjects
- Requirement to imbed data protection by default in the design of operation of all services.

2.7 What is the difference between personal, sensitive and non-sensitive data?

Personal data refers to any information referring to an identified or identifiable natural person. An Identifiable Natural Person is a person who is:

- Identified by an identifier such as a name, an identification number, location data or an online identifier
- Identified by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive data refers to matters such as ethnic/cultural background of the pupil and religion. Express written consent is required from parents/guardians before such information is recorded. The obvious time for seeking such consent is upon enrolment.

Non-sensitive data relates to PPSN, name and address. Parents/guardians are advised by way of notice as to how and why this data is recorded and for how long it is retained.

2.8 What rights have Data Subjects?

PAM

The Data Protection legislation enables parents and pupils over 18 years to enquire whether schools are processing information about them and, if so, to access that information. It enables these individuals to ensure that personal information about them is being fairly processed and if not, to have that personal information rectified or erased.

2.9 Who is the Data Controller in a school?

The data controller in a school is the BoM.

2.10 What is the role of a Data Protection Officer (DPO)?

The role of the DPO is to communicate, advise, guide, represent and record. The purpose of a DPO is to assist an organisation in monitoring internal compliance with the GDPR. They will be the cog in in an organisation's data governance structure and will enable compliance through the implementation of accountability principles. The DPO will act as a mediator between an organisation and key stakeholders, such as the supervisory authorities and data subjects. There is a mandatory list of tasks for which the DPO is responsible. These tasks are outlined in article 39 of the GDPR, and have been echoed in the Data Protection Bill 2018.The DPO advises the controllers and processors. The DPO also involves awareness raising and training of relevant staff. The DPO is also the contact point with the Data Protection Commissioner and would also be contacted in the event of a data breach. A clear conflict of interest arises if the DPO is also the Data controller.

2.11 Does your school need to appoint a DPO?

Under GDPR you must appoint a DPO if you are a pubic body. As ETB schools are public authorities, they are obligated to appoint a DPO. Schools other than ETBS are at present not legally obliged to appoint a DPO. Even if you don't have to appoint a DPO, schools still have to comply with the requirements of GDPR. Schools not obligated to appoint a DPO can still appoint one if they so choose. Schools can share the services of a DPO for a group/cluster. Section 33 of the Bill states that the Minister for Justice and Law Reform may, following consultation with such other Minister for Government, require controllers or processers in that particular sector to designate a data protection officer.

2.12 Who is (are) the Data Processor(s) in a school?

The Data Processor(s) is/are any person or persons given access to personal data held by the Data Controller for processing. This would include agencies such as Aladdin, Databiz etc. who process information on behalf of the Data Controller. The data controller outsources the data to be processed to a data processor.

2.13 What is meant by Data Processing?

Data Processing is carrying out any of the following actions with information:

a. Collecting
b. Recording
c. Organising
d. Structuring
e. Storing
f. Adapting
g. Altering
h. Retrieving
i. Consulting
j. Using
k. Disclosing
l. Disseminating
m. Aligning or combining
n. Restricting
o. Erasing
p. Destroying

2.14 What is meant by Fair Processing?

PAM

Fair Processing means that data is only processed with

a. The consent of the Data Subject

Or

b. A legitimate basis e.g. statute, contract or legitimate interest

And

c. Processing must be proportionate and fair.

2.15 WHAT IS MEANT BY CONSENT?

PAM

Where consent is the basis for provision of personal data (e.g. data required to join sports team/ after-school activity/or optional school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes. Each 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.

To ensure that the school's practices are open and transparent and to obtain data fairly, the data subject must, at the time the personal data is being collected, be made aware of:

a. the name of the data controller (i.e. school BoM)
b. the purpose/rationale for collecting the data and any secondary uses of their personal data which might not be obvious to them
c. the persons or categories of persons to whom the data may be disclosed e.g.
    i. DES
    ii. other third parties operating in the education and welfare sphere e.g. NCSE, NEWB, NEPS, SESS, the HSE, TUSLA, An Garda Síochána
    iii. other third parties with whom the school contracts, such as cloud-based school administration software companies, accountants, insurance companies, lawyers, etc.
d. whether replies to questions asked are obligatory and the consequences of not providing replies to those questions
e. the existence of the right to access their personal data
f. the right to rectify their data if inaccurate or processed unfairly
g. any other information which is relevant so that processing may be fair and to ensure that the data subject has all the information that is necessary to facilitate their awareness of how their data will be processed.

2.16 HOW DOES A SCHOOL ENSURE THAT ITS DATA IS ACCURATE?

In order to keep data accurate, complete and up-to-date, school BoMs must:

- Take reasonable steps to ensure the accuracy of the personal data they have obtained
- Consider whether it is necessary to update the information, especially if the data is time-sensitive (i.e. likely to become inaccurate over time unless it is updated)
- Verify that manual and computer procedures ensure high levels of data accuracy.
- Assess how to keep personal data up-to-date. Is this done on a periodic basis (e.g. once a year or on renewal of a contract)?

It is also in the school's interest to ensure accurate data for reasons of efficiency and effective decision-making.

2.17 What about transferring data to another primary school or to a secondary school?

Section 28 of the Education Welfare Act 2000 allows for personal data to be transferred to other schools, the DES, the National Council for Special Education, and the Child and Family Agency (Tusla). Principals of primary schools furnish secondary schools (which have confirmed enrolment of the pupils concerned) with 'Education Passports', which include a copy of the end-of-year report card and information from standardised literacy and numeracy assessments completed in sixth class.

2.18 What about transferring data to a data processing company?

PAM

If a school obtains personal information for a particular purpose, you may not use the data for any other purpose, and you may not divulge the personal data to a third party, except in ways that are compatible with the specified purpose. A key test of compatibility is whether you use and disclose the data in a manner such that those who supplied the information would expect it to be used and disclosed.

Note that transfers of personal data to agents of the school, who are carrying out operations upon the data on behalf of the school and not retaining it for their own purposes, do not constitute 'disclosures' of data for the purposes of the Act. Examples of such transfers would include the transfer of staff data to a separate payroll company for payroll administration purposes, and the transfer of personal data from a school to a school administration agent e.g. Aladdin, Databiz, TextaParent etc.

Schools should be able to answer Yes to the following questions:-

a. Is the data used only in ways consistent with the purpose or purposes for which it is kept?
b. Is the data disclosed only in ways consistent with that purpose or purposes?

2.19 Who can request data from a school?

PAM

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. PAM

Data protection legislation allows exemptions in relation to schools providing, or 'disclosing', information to:

a. The Gardaí
b. The Revenue Commissioners
c. Department of Social Protection (DSP)
d. Applications on foot of a court order
e. Tusla (Child and Family Agency).

If you are in doubt as to whether to release data or not, always seek legal advice or advice from the Office of the Data Protection Commissioner.

2.20 What practical steps should schools take to ensure compliance with GDPR?

PAM

In order to comply with GDPR, every BoM should ensure that:

- They are aware of what data they currently hold and what data they are processing on an on-going basis
- Their relevant staff are fully trained for their roles in relation to GDRP
- All school staff are fully aware of the importance of data protection and that the school is a Data Protection Sensitive and Aware institution
- That all relevant policies and procedures are in place and embedded.

On a practical level, this will require the BoM to consider the following areas (see **PAM** for further details of each area):

- Data audit
- Staff training
- Embedding of a data protection culture
- Policies, agreements and notifications
- Administration forms
- Procedures and routines.

2.21 What additional wording needs to be added to Enrolment Forms?

All schools use administration forms e.g. enrolment forms, BoM election ballot papers, permission to use photographs of a child etc. to assist in the smooth running of the school. In the main these forms gather information which is then processed by the BoM or by a Data Processor on behalf of the BoM. In order to reassure Data Subjects that the BoM is following fair processing procedures, as is required by the data protection legislation, it is important to ensure that all such forms contain a clear and specific rationale for the collection of such data. Data Subjects have the right to know:

1. what data is being processed
2. the reasons for that processing
3. the name of the Data Controller who is responsible for the processing of their Data.

The wording for such documents should reflect the conditions outlined in Section 2A of the Data Protection Legislation. These are outlined in the IPPN document "Fair Processing" **PAM**

2.22 What access have Data Subjects to notes written by principals and teachers?

While schools other than ETB schools are not subject to the Freedom of Information Acts 1997-2003, they are subject to data protection legislation. Data Subjects have a right to access all data relating to them. This includes written notes. It therefore behoves all principals and teachers to exercise caution when recording such notes. They are advised to record all such notes as though the Data Subject were looking over their shoulder. Such notes should be factual and, where opinions are stated, they should be capable of being substantiated.

2.23 What if data is disclosed unintentionally or hacked?

Data controllers are under a specific obligation to take appropriate measures to protect the security of such data (Section 2(1)[d]).

A data breach occurs where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form. In that instance, the data controller must inform the Office of the Data Protection Commissioner within 72 hours of the breach. In instances where the data controller believes there is a serious risk to the rights and freedoms of data subjects, they must give immediate consideration to informing the data subjects affected. Such information permits data subjects to consider the potential consequences and to take appropriate measures. In appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions, etc.

All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to the relevant data controller as soon as the data processor becomes aware of the incident. All data processors must be aware of this and the message must be reinforced through training. In case of doubt, in particular any doubt related to the adequacy of technological risk-mitigation measures, the data controller should report the incident to the Office of the Data Protection Commissioner within 72 hours of the breach.

2.24 What support is available to schools to ensure compliance with their data protection obligations?

a. Office of the Data Protection Commissioner website (Click here for information)
b. IPPN Resource Bundle
c. IPPN Leadership Support Team

2.25 How long must schools retain data

PAM

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	**Retention Periods**
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	Retention Periods
Contract of employment Teaching Council registration Vetting records	Retention for duration of employment + 7 years
Accident/Injury at work reports	(6 years to make a claim against the school plus 1 year for proceedings to be served on school)
BoM Records	**Retention Periods**
BOM agenda and minutes CCTV recordings	Indefinitely 28 days normally. In the event of criminal investigation – as long as is necessary
Payroll & taxation	Revenue require a 6-year period after the end of the tax year
Invoices/receipts	Retain for 7 years
Audited accounts	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.	

2.26 What about CCTV?

PAM

All schools must have a CCTV Policy in place which covers the following areas:-

- Introduction
- Purpose
- Scope
- General principles
- Justification
- Location
- Covert surveillance
- Notification and signage
- Retention and storage
- Access
- Responsibilities
- Security companies
- Implementation and review.

2.27 What is a Privacy Impact Statement?

PAM

Before a school installs a new CCTV system, it is recommended that a documented privacy impact assessment is carried out. A privacy impact assessment means the BoM should carry out a risk assessment and list all the potential risks of personal data breaches and document how the risks will be addressed. A school which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the data protection legislation. This is an important procedure to adopt as a contravention may result in action being taking against a school by the Office of the Data Protection Commissioner, or may expose a school to a claim for damages.

2.28 Data Protection Policy

PAM

It is advisable for all schools to have a Data Protection Policy which defines the school's use of data and its adherence to best data processing practice. However, it is of little use unless its contents are known and implemented by all staff who are involved with any form of personal data collecting or processing. Please click **PAM** to download a draft School Data Protection Policy.

2.29 Website Privacy Statement

PAM

The Data Protection Commissioner recommends that a Privacy Statement be placed in a reasonably obvious position on the website homepage.

3 RESOURCES AVAILABLE

3.1 PAMs IN THIS RESOURCE BUNDLE

- The 8 Rules of Data Protection
- Your Rights as a Data Subject
- Fair Obtaining and Processing
- Consent
- Draft Third Party Service Agreement
- Data Retention Periods for Schools
- Draft CCTV Policy for Schools
- Draft Privacy Impact Statement
- Draft Data Protection Policy for Schools
- Draft Website Privacy Statement
- Draft Data Access Request Form
- Practical Steps for GDPR

3.2 USEFUL WEBSITES:

- www.dataprotection.ie
- www.dataprotectionschools.ie
- www.gdpr-info.eu