Edmund Rice College
Generosity Compassion Faith Courage

Data Protection Policy of Edmund Rice College Phoenix Park

School Details

Address:	Phoenix Park Racecourse, Parkway Road, Navan Road, Castleknock, Dublin 15.
Roll Number:	68306h
School Patron:	The Edmund Rice Schools Trust

Ratification and Review

Date of ratification: 22/04/2026

Chairperson of the Board of Management	Principal
Signed:	

Date of next review: April 2028

Iontaobhas Scoileanna Éamainn Rís
Edmund Rice Schools Trust

Table of Contents

Mission statement

Our mission at Edmund Rice College is to foster a culture of generosity and acceptance where each person has both the faith and courage to speak and act with compassion. We are committed to the holistic development of each child and will support them through their spiritual, moral, intellectual, social, emotional and physical development, while honouring their diverse learning styles. To recognise and develop each person's sense of self worth which, will foster a genuine interest and concern for others in the wider community and in the world in which we live. We recognise and respect the role of parents as primary care givers and in our capacity as educational professionals, we will work together to guide and support students to become responsible, accountable and caring citizens.

Vision statement

At Edmund Rice College we strive to further develop a community that welcomes and nourishes our gospel-based values, that prepares our children for life long learning and is a place where friendships are formed.

To achieve our vision at Edmund Rice College we aim:

- To nourish Christian values as a Catholic Community. To plan, organise and celebrate as a Eucharistic community.
- To challenge and encourage our students to achieve their personal best in all endeavours.
- To provide a stimulating, happy and secure environment where each child, teacher and adult is valued.
- To welcome, respect and value people in all faiths and cultures.
- To provide a caring community where little things matter.

Introduction

This policy has been formulated in consultation with the staff, parents and Board of Management of Edmund Rice College Phoenix Park, in order to comply with the EU General Data Protection Regulation (GDPR) and Irish Legislative Acts.

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 General Data Personal Regulation (GDPR).

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.

Edmund Rice College are conscious to plan carefully when gathering personal data so that we build in the data protection principles as integral elements of all data operations in advance.

This policy outlines the manner in which personal data is collected, stored, protected and destroyed by the school. Data will be stored securely so that confidential information is protected in compliance with relevant legislation.

Links between the schools' GDPR policy and School Ethos

Edmund Rice College Phoenix Park seeks to:

- Enable students 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 students, 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.

Data Protection Principles

The school BoM is a ***data controller*** of *personal data* relating to its past, present and future staff, students, 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 data fairly

Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous school, if applicable. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students, 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.
(See: Appendix 1)

2. Obtain consent

Where consent is the basis for provision of personal data, (e.g. data required to join sports teams/ 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. Edmund Rice College Phoenix Park 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. (See: Appendix 2)

3. Retain data for specific/lawful purposes

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. Storage Limitations and Access.

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. Portable devices storing personal data (such as laptops) are encrypted and password protected. 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 Accurate Data

Keep Personal Data accurate, complete and up to date.
Students, 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.

6. Data Minimisation

Ensure that data collected is adequate, relevant and not excessive.
Only the necessary amount of information required to provide an adequate service will be gathered and stored.

7. Retain data for specified durations

Retain data 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 3)

8. Process Data Requests

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(s) for which it is held (See: Appendix 4).

Policy 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, students and their parents/guardians about how their data will be managed.

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 school handles or processes their *Personal Data* in the course of their dealings with the school.

Disclaimer

By enrolling your child in and/or by attending Edmund Rice College Phoenix Park, you acknowledge and agree to the collection and processing of personal information by 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).

The Data Controller is the Board of Management of the school.

The Data Subject is an individual who is the subject of the personal data.

Data Processing is 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;

A Data Processor is 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 (e.g. Aladdin; school accounting / wages processors).

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 is 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.

GDPR Policy 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 students 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. Edmund Rice College Phoenix Park sends, by post, a copy of a child's birth certificate, as provided by the National Council for Curriculum and Assessment, to the principal of the Post-Primary School in which the pupil has been enrolled.

Where reports on pupils which have been completed by professionals, apart from Edmund Rice College Phoenix Park staff, are included in current pupil files, such reports are only passed to the post-primary 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 students 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 and Skills, 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 and Skills, 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)

Forms of Personal Data

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

Staff records

Categories of 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 being probated. 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 and Skills, 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:

- Manual records are kept in a secure, locked filing cabinet in the main administrative office/ principal's 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.
- 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.

Student records

Categories of 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 (e.g. special educational needs, health issues,) which may apply;
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student;
- Psychological, psychiatric and/or medical assessments;
- Attendance records;
- Photographs and recorded images of students (including at school events and noting achievements) are managed in line with the accompanying policy on school photography;
- Academic record – subjects studied, class assignments, examination results as recorded on official school reports;
- Records of significant achievements;
- 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, (Note: it is advisable to inform parents that a particular incident is being recorded);
- 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.

Purpose:

- to enable each student to develop to his/her full potential;
- to comply with legislative or administrative requirements;
- to ensure that eligible students 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 student;

- photographs and recorded images of students 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.
- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirement for attendance at Primary School.
- to ensure that any student 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 and Skills, the National Council for Special Education, Tusla, and other schools, etc. in compliance with law and directions issued by government departments
- to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/references to second-level educational institutions.

Board of Management records

Categories of 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.

Other Records: Creditors

Categories of 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:
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.

CCTV images/recordings

CCTV is installed in Edmund Rice College Phoenix Park.

- Cameras are installed externally around the perimeter of the main building
- Cameras are also installed on the corridors adjacent to student toilets.

These CCTV systems may record images of staff, students and members of the public who visit the premises.
The viewing station for external CCTV cameras is in the school's central communications office. This office is locked at all times. A log is kept of all persons authorised to examine footage from the CCTV system and this is done under the Principal's supervision only. In each instance where there is cause to review CCTV footage, the following details are recorded in the log

- Date / time of access
- Cameras viewed
- Date/time of footage reviewed
- Any footage extracted to an external hard drive.

Images/recordings may be viewed or made available to An Garda Síochána pursuant to Data Protection Acts legislation.

For the sixteen internal CCTV cameras, a live feed is available directly to Senior Management'swork mobile phone. Access to the data on Management's phone requires dual authentication. In addition to the live feed, these cameras record data for 6 hours. This data is then overwritten and lost. The Principal keeps a record of access to these cameras.

Purposes:
Safety and security of staff, students and visitors and to safeguard school property and equipment.

Security:
Access to images/recordings is restricted to the Principal (DLP) of the school. Recordings are retained for 28 days, except if required for the investigation of an incident.

Examination results:

The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual and continuous assessment results, Diagnostic Test 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 guardians 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 and Skills, the National Council for Curriculum and Assessment and other schools to which a pupil will move to.

Enrolment forms:
Enrolment forms for prospective students are submitted in hard-copy to the school office or through email. Enrolment forms submitted through email are printed and processed. This process is completed by the end of October each year.

When a student is accepted to Edmund Rice College and enrols as a student:

- Enrolment forms are stored as part of their student file.
- They are stored securely for the duration of the student's time in the college.
- They are shredded one year after completion of their time in the college.

When a student submits an enrolment form to Edmund Rice College and does not secure a place:

- Enrolment forms are stored securely and retained for one year. This is to ensure the student file is available should a place become available at a later date.
- After the file has been retained for one year and the student has not enrolled in the college, the enrolment form is shredded.

Other policies in relation to data protection

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:

- Child Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Enrolment Policy
- ICT Acceptable Usage Policy
- Assessment Policy
- Special Educational Needs' Policy
- Critical Incident Policy
- Attendance Policy

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 (See: Appendix 5)

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*).** Edmund Rice College Phoenix Park 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 after having become aware of the breach.
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 (See: Appendix 4)
Request must be responded to within one month. An extension may be required (e.g. over holiday periods etc.)
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.

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 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 the schools data protection responsibilities and procedures.

The following personnel have **responsibility** for implementing the Data Protection Policy:

Name	Responsibility
Board of Management	**Data Controller**
Principal	**Implementation/Monitoring Policy**
Teachers / Staff	**Implementation of Policy**

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 and Skills or TUSLA), legislation and feedback from parents/guardians, students, 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

APPENDICES

Appendix 1: Fair Processing
Appendix 2: Consent
Appendix 3: School Record Retention Table
Appendix 4: Personal Data Access Request Form
Appendix 5: Personal Rights as a Data Subject
Appendix 6: The 8 Rules of Data Protection

Appendix 1: Fair Processing

Fair Processing of personal data

Section 2A of the Acts details a number of conditions, at least one of which must be met, in order to demonstrate that personal data is being processed fairly. These conditions include that the data subject has consented to the processing, or that the processing is necessary for at least one of the following reasons:

1. The performance of a contract to which the data subject is party, or
2. In order to take steps at the request of the data subject prior to entering into a contract, or
3. In order to comply with a legal obligation (other than that imposed by contract), or
4. To prevent injury or other damage to the health of the data subject, or
5. To prevent serious loss or damage to the property of the data subject, or
6. To protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged, or
7. For the administration of justice, or
8. For the performance of a function conferred on by or under an enactment or,
9. For the performance of a function of the Government or a Minister of the Government, or
10. For the performance of any other function of a public nature performed in the public interest by a person, or
11. For the purpose of the legitimate interests pursued by a data controller except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject

Fair processing of *sensitive* personal data:

If processing sensitive data, you must satisfy the requirements for processing personal data set out above along with at least one of the following conditions (set out in section 2B of the Acts):

1. The data subject has given explicit consent, or
2. The processing is necessary in order to exercise or perform a right or obligation which is conferred or imposed by law on the data controller in connection with employment, or
3. The processing is necessary to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in

a case where consent cannot be given, or the data controller cannot reasonably be expected to obtain such consent, or

4. The processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld, or
5. The processing is carried out by a not-for-profit organisation in respect of its members or other persons in regular contact with the organisation, or
6. The information being processed has been made public as a result of steps deliberately taken by the data subject, or
7. The processing is necessary for the administration of justice, or
8. The processing is necessary for the performance of a function conferred on a person by or under an enactment, or
9. The processing is necessary for the performance of a function of the Government or a Minister of the Government, or
10. The processing is necessary for the purpose of obtaining legal advice, or in connection with legal proceedings, or is necessary for the purposes of establishing, exercising or defending legal rights, or
11. The processing is necessary for medical purposes, or
12. The processing is necessary in order to obtain information for use, subject to, and in accordance with, the Statistics Act, 1993, or
13. The processing is necessary for the purpose of assessment of or payment of a tax liability, or
14. The processing is necessary in relation to the administration of a Social Welfare scheme

Appendix 2: Consent

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:

1. the name of the data controller (i.e. School BoM)
2. the purpose/rationale for collecting the data and any secondary uses of their personal data which might not be obvious to them
3. the persons or categories of persons to whom the data may be disclosed e.g.
    - DES
    - other third parties operating in the education and welfare sphereg. NCSE, TUSLA, NEPS, SESS, the HSE,TUSLA, An Garda Síochána
    - other third parties with whom the School contracts, such as cloud-based school administration software companies, accountants, insurance companies, lawyers, etc.
1. whether replies to questions asked are obligatory and the consequences of not providing replies to those questions
2. the existence of the right to access their personal data
3. the right to rectify their data if inaccurate or processed unfairly
4. 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

Where you use application forms or standard documentation in school for enrolment or other purposes, you should explain your purposes/uses etc. clearly on such forms or documentation

No age limit is associated with consent. However, it is important that the data subject appreciates the nature and effect of such consent. Therefore, different ages might be set for different types of consent. Where a person is unlikely to be able to appreciate the nature or effect of consent, by reason of physical or mental incapacity or age, then a parent, grandparent, uncle, aunt, brother, sister or guardian may give consent on behalf of the data subject. These are the only circumstances in which a third party may give consent on behalf of a data subject

Fair Obtaining of Data: Test Yourself

When people are giving you information, you should be able to answer YES to the following questions:

1. Do they know what information you will keep about them?
2. Do they know the purpose for which you keep and use it?
3. Do they know the people or bodies to whom you disclose or pass it?

In general, the fair obtaining principle requires that every individual about whom information is collected for holding will be aware of what is happening

Appendix 3: School Record Retention Table

Record Type	Retention Period
Student Records	
School Register/Roll Book	Indefinitely
Application & Enrolment Forms	Hold until pupil is 25 years
Disciplinary Notes	Never Destroy
Test Results - Standardised	Never Destroy
Psychological Assessments	Never Destroy
SEN files/IEP's	Never Destroy
Accident/Incident Reports	Never Destroy
Child Protection Reports/Records	Never Destroy
Exam Appeal Records	Hold until pupil is 25 years
Interview Records	
Application Forms	18 months from close of competition plus 6 months in case Equality Tribunal needs to inform school that a claim is being taken
Interview Scores & Feedback	As Above
Interview Board List of Members	As Above
Staff Records	Duration of employment + 7 years
Contract of Employment/Appointment	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 the school
Teaching Council Registration	As above
Vetting Records	As above
Accident/injury at work Reports	As above

BoM Records	
BoM Meeting Agenda and Minutes	Indefinitely
CCTV Recordings	28 days normally. In the event of criminal investigation – as long as is necessary
Payroll & Taxation	Revenue requires a 6-year period after the end of the tax year
Invoices & Receipts	Retain for 7 years
Audited Accounts	Indefinitely
Agreed Report	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.

Data that becomes obsolete will be shredded and/or deleted permanently from school files and computer drives.

Appendix 4: Personal Data Access Request Form

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 (eg. 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 o	**Former Pupil** o	**Current Staff Member** o	**Former Staff Member:** o
Name of Pupil:		Date of Birth of Pupil:	
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 Edmund Rice College Phoenix Park 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 (e.g. if requesting images/recordings made by CCTV, please state the date, time and location of the images/recordings as otherwise it may be very difficult or impossible for the school to locate the data)
This **Access Request** must be accompanied with a copy of photographic identification e.g., passport or drivers licence. 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:…….

Please return this form to the relevant address:
To: The Chairperson Board of Management, Edmund Rice College Phoenix Park.

Appendix 5: Personal Rights as a Data Subject

1. Right to have your data processed in accordance with the Data Protection Acts: To have your personal information obtained and processed fairly, kept securely and not unlawfully disclosed to others.

2. Right to be informed: To know the identity of the data controller and the purpose for obtaining your personal information

3. Right of access: To get a copy of your personal information

4. Right of rectification or erasure : To have your personal information corrected or deleted if inaccurate

5. Right to block certain uses: To prevent your personal information being used for certain purposes

6. Right to have your name removed from a direct marketing list: To stop unwanted mail

7. Right to object: To stop some specific uses of your personal information

8. Employment rights: Not to be forced into accessing personal information for a prospective employer

9. Freedom from automated decision making: To have a human input in the making of important decisions relating to you

10. Rights under Data Protection and Privacy in Telecommunications Regulations: To prevent your phone directory entry details from being used for direct marketing purposes

Appendix 6: The 8 Rules of Data Protection

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**
8. **Give a copy of his/her personal data to that individual on request**

DATA BREACH
PROTOCOL POLICY

Voluntary Secondary School Procedure for Handling a Personal Data Breach

Disclaimer: This document is provided as a resource to assist schools. While every effort has been made to ensure the accuracy of the informaCon provided, schools are advised to exercise common sense, consult up to date circulars, legislaCon, case-law, and/or guidelines from relevant agencies. Where queries arise, schools are urged to obtain Cmely advice from their professional advisers. This document does not consCtute legal advice.

Procedure for Handling a Personal Data Breach

1. Scope and Purpose

1.1. The purpose of this procedure is to guide the school's response in the event of a personal data breach.[1]

1.2. This procedure will be:

(a) highlighted to staff at induc7on and at periodic staff mee7ngs/ training.

(b) circulated to all appropriate data processors. Data processors are required to immediately contact the school should they become aware of a breach of personal data that is being processed by them on behalf of the school.

1.3. This procedure should be understood and applied in conjunc7on with other relevant school policies and procedures (most notably the school's Data Protec7on Policy).

1.4. The school's priority, in response to any personal data breach, will be to take prompt ac7on to minimise any risk to individuals and their personal data.

1.5. In nearly all circumstances, an effec7ve breach response by the school will require each of the areas of ac7on (listed below) to be progressed in parallel with each of the others.[2]

- Confirm that a breach has occurred and inves7gate the facts surrounding it.
- Communicate as necessary with stakeholders, advisors and others.
- Implement ac7ons to contain and mi7gate the breach (including data retrieval where possible).

[1] The data protec7on legisla7on changed on 25th May 2018 with the coming in to force of the GDPR and the imposi7on of a new set of legal obliga7ons on data controllers including mandatory no7fica7on of data breaches in certain circumstances - as summarised in Appendix 3.

[2] The fact that these areas of ac7on are presented sequen7ally in this procedure should not be taken to imply a sequen7al approach to managing a personal data breach.

- Assess the extent of the risk to those affected and the likelihood of these risks materialising.
- No7fy, as appropriate, the Data Protec7on Commission (DPC) and the affected data subjects.

2. Causes and Impact

2.1. **Causes** A personal data breach can come about as a consequence of either a deliberate ac7on or an accident. And while the term 'data breach' is o]en used synonymously with 'cyber-a^ack', not all cybera^acks result in data breaches, and it is certainly the case that not all data breaches are the result of cybera^acks. In fact, most personal data breaches in schools (as elsewhere) occur as a consequence of human error. Common causes of data breaches include:

- Loss or inappropriate disposal of paperwork or any device containing data.
- Poor access controls allowing unauthorised use or access.
- The], burglary, mugging.
- Equipment failure and inadequate system back-ups.
- A disaster such as flood or fire.
- Phishing or blagging (where informa7on is obtained by decep7on or spoofing).
- Malicious a^acks such as hacking or ransomware a^ack.

2.2. **Effects of breaches on individuals** Personal data breaches can have adverse effects on individuals and lead to physical, material, and non-material damages. These can include causing embarrassment, distress, and/ or humilia7on. Other adverse effects to individuals may include: *loss of control over their personal data, limitaCon of their rights, discriminaCon, idenCty theK or fraud, financial loss, unauthorised reversal of pseudonymisaCon, damage to reputaCon, loss of confidenCality of personal data protected by professional secrecy, significant economic or social disadvantage.*[3]

2.3. **Effects of breaches on the school** Personal data breaches can also be damaging to the school as they can result in:

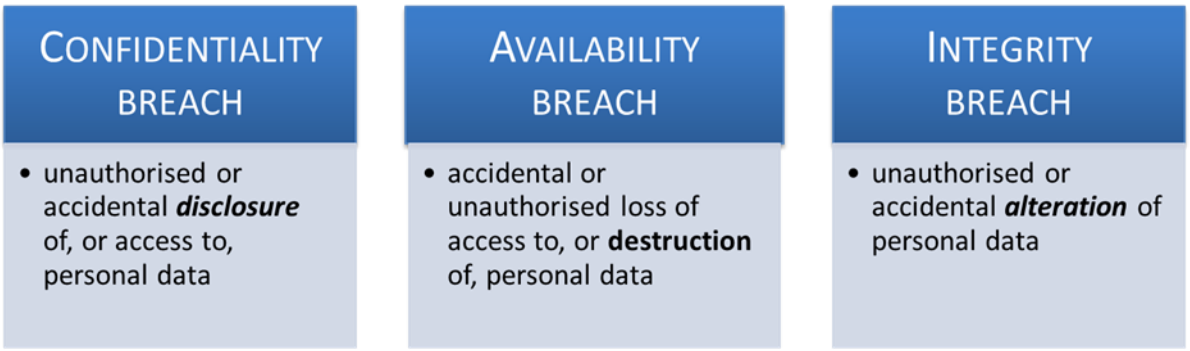
- Damage to the rela7onship of trust built with stakeholders (students, parents, staff, trustees and members of wider community).
- Consump7on of school resources in addressing inves7ga7on, mi7ga7on, remedia7on and communica7on issues.
- Loss of, or damage to, personal data essen7al to the administra7on of the school.
- Administra7ve sanc7ons and fines in accordance with the provisions of Data Protec7on legisla7on.
- Exposure to poten7al li7ga7on.

3. DefiniPon and InvesPgaPon

3.1. **DefiniPon of a personal data breach** A personal data breach is a breach that impacts on personal data (i.e.

[3] Page 8, *ArCcle 29 Working Party Guidelines on Personal Data Breach NoCficaCon under RegulaCon 2016/679 (WP250).*

informa7on that relates, directly or indirectly, to an iden7fiable person).[4] A personal data breach occurs whenever the confiden7ality, availability or integrity of this type of informa7on is compromised.



3.2. All staff should be able to recognise a personal data breach and understand that personal data doesn't need to have been disclosed to a third party; it may also have been altered, corrupted, lost or destroyed.[5]

3.3. The informa7on received in the early stage of a breach of personal data is not always accurate or complete. Some degree of inves7ga7on may be needed to rapidly establish whether the integrity of personal data under the school's control has been compromised.

3.4. It may be appropriate to gather together a small team to assess any poten7al exposure/loss and iden7fy appropriate containment/mi7ga7on/remedia7on measures.[6]

3.5. The scope of any inves7ga7on should reflect the informa7on requirements set out in the data protec7on legisla7on. GDPR Ar7cle 33(5) requires schools to document all personal data breaches (regardless of level of risk or impact). The "Data Security Breach Incident Report" form (Appendix 1) provides a suitable template.[7]

3.6. Any ini7al inves7ga7on of a data breach might focus on clarifying the following informa7on:

(a) Date/7me of ini7al communica7on of breach, including details of who reported the ma^er.

(b) Details of what is known/suspected at this ini7al stage.

(c) Details of what system/data is involved.

(d) Any tasks necessary to confirm the occurrence and extent of the breach.

(e) An ini7al assessment of any risks to the rights and freedoms of natural persons.

(f) List of poten7al follow-on ac7ons (inves7ga7on, containment, mi7ga7on, recovery, etc).

---

[4] While data breaches can happen to any kind of informa7on, GDPR is only concerned with personal data. GDPR defines a personal data breach as *A breach of security leading to the accidental or unlawful destrucCon, loss, alteraCon, unauthorised disclosure of, or access to, personal data transmiYed, stored or otherwise processed*.

[5] The school should provide staff with access to relevant informa7on and training as appropriate.

[6] All staff and all data processors and/or joint data controllers are required to give all necessary assistance to the Principal and this team.

[7] Regardless of whether (or not) a decision is made to no7fy the DPC, all documenta7on rela7ng to a personal data breach, including but not limited to the documenta7on required by GDPR Ar7cle 33(5), should be stored in the school's GDPR Accountability file.

(g) Summary of tasks assigned to relevant staff and others (e.g. IT service providers etc).

(h) Details of all likely communica7ons, including any no7fica7ons to DPC and affected individuals.

3.7. In appropriate circumstances, considera7on may need to be given to retaining an IT forensics specialist.

4. CommunicaPons[8]

4.1. **Staff**

(a) All staff should understand the need to report a suspected breach to senior management in a 7mely manner. Early recogni7on and communica7on is essen7al if the 72 hour limit for no7fica7on to the DPC is be observed and the rights of data subjects are to be protected.

(b) All staff should be aware that the 72 hour 7me period does not differen7ate between working and non-working days[9] and commences from the moment the data controller becomes aware of a data breach.[10]

4.2. **Board of Management** The Principal must report all personal data breaches to the Board of Management.

[11] The Board should agree a clear protocol with the Principal around the 7ming of these communica7ons.

For example,

(a) for any data breaches that are assessed as "low risk", it might be agreed that these are rou7nely no7fied to the Board at its termly business mee7ng.

(b) for a breach assessed as "high risk", it might be agreed that the Principal would inform the Chairperson at the earliest opportunity.[12]

4.3. **An Garda Síochána**

---

[8] Important Note: the school should avoid including any personal data in the documenta7on or informa7on that is being shared as part of these communica7on processes. While the recipients will generally be bound by a duty of confiden7ality, there is usually no purpose or benefit to sharing the actual personal data that has been breached. For example, the DPC generally advises that it does not want controllers to include any affected personal data when filing a mandatory breach no7fica7on. Similarly, while a school's Board of Management may choose to review a personal data breach in detail in order to fulfil its responsibili7es as data controller, this func7on will rarely if ever require the Board to access the personal data itself.

[9] For example, if the school becomes aware of a data breach at 9am Friday, then a no7fica7on (if required) will need to be filed no later than Monday 9am.

[10] The school can be regarded as having become "aware" whenever there is a reasonable degree of certainty that a security incident has led to personal data being compromised.

[11] The Board of Management is the designated Data Controller and, as such, should have an understanding of the key data protec7on issues that relate to the school's opera7on. It is therefore recommended that "Data Protec7on" is included as a recurring item on the agenda of Board mee7ngs. The fact that the incidence of data breaches must be communicated to the Board does not necessitate the sharing of any personal data with the Board as part of this repor7ng process.

[12] Early no7fica7on will allow the Chairperson to act in a 7mely ac7on (e.g. to convene an emergency mee7ng of the Board where this is deemed necessary. In certain circumstances it may be appropriate to give considera7on to the prepara7on of a press release.).

(a) Depending on the nature of the personal data breach, and par7cularly where sensi7ve personal data may be at risk, assistance might be sought from An Garda Síochána.

(b) Where data has been accessed without authority, the ma^er shall be reported immediately to An Garda Síochána.[13]

(c) Where data has been "damaged" (as defined in the Criminal Jus7ce Act 1991, e.g. as a result of hacking), the ma^er must be reported to An Garda Síochána. Failure to do so will cons7tute a criminal offence in itself ("withholding informa7on") pursuant to sec7on 19 Criminal Jus7ce Act, 2011. The penal7es for withholding informa7on include a fine of up to €5,000 or 12 months' imprisonment on summary convic7on.

4.4. **Insurance Company** Where there is deemed to be risk associated with a personal data breach then the school should contact its insurance company to advise them that there has been a security incident.

4.5. **Legal Advisors** The school may no7fy its legal advisors and advise them that there has been a security breach for the purposes of obtaining legal advices and defending, compromising or otherwise se^ling li7ga7on.

4.6. **Others** Where appropriate (depending upon the nature of the data put at risk, e.g. if it contains sensi7ve informa7on rela7ng to children or vulnerable persons, such as child protec7on or safeguarding ma^ers) contact may be made with other bodies such as the HSE, TUSLA, financial ins7tu7ons, etc.

5. Containment and Recovery

5.1. The school will immediately seek to contain the incident (insofar as that is possible) and take all feasible steps to mi7gate any further exposure or risk.

5.2. Depending on the nature of the breach/threat to personal data, appropriate containment ac7ons may include:

- a quaran7ne of manual records storage area/s and other areas
- immediately retrieving paper documents from any unintended recipients
- direc7ng staff not to access PCs, networks, devices etc.
- changing passwords for affected applica7ons, devices, systems or rooms
- advising users to change their passwords
- ac7ng to suspend user access and/or accounts
- an audit of records held on backup server(s)
- contac7ng any recipient of an email sent in error and asking them confirm dele7on
- immediately disabling any lost or stolen electronic devices
- remotely loca7ng, disabling and/or dele7ng data stored on a mobile device
- restoring a database or system from a back-up
- disabling network or system access
- no7fying staff and/or Processors to do (or refrain from doing) something

[13] "If you believe your account or your network has been hacked because you can't get access or you have no7ced unusual ac7vity, you should report it to your local Garda sta7on". Garda Cybercrime advice h^ps://www.garda.ie/en/Crime/Cyber-crime/ (accessed March 2020).

- ensuring that ac7ons don't inadvertently compromise the integrity of any inves7ga7on.

5.3. Where the security incident relates to an IT system and/or electronic data, 7mely contact may need to be made with the school's IT service providers(s) and their advices and assistance sought in rela7on to appropriate measures of containment, quaran7ne, preserva7on of data and logs[14] etc.

5.4. For serious incidents the school may seek input from an independent expert. Independent exper7se can help to determine the source and scope of the breach, collect and analyse evidence, and outline remedia7on steps.

6. Risk Assessment

6.1. The school must undertake an assessment in rela7on to the risk(s) arising from any personal data breach

i.e. <u>is the personal data breach likely to result in a risk to the rights and freedoms of natural persons?</u>[15]

6.2. In assessing the level of risk, the school must focus on the risk to the data subjects e.g. (i) What are the poten7al adverse consequences for individuals? [16] (ii) How serious are these consequences?
(iii) How likely is it that these consequences will materialise?

6.3. If the data breach concerns the data of children or other vulnerable individuals, then this will inevitably heighten the level of risk.

6.4. The risk assessment process must provide an outcome that allows the school to classify the level of risk associated with the breach, as either:

A. There is **no risk <u>or</u> any risk is unlikely to materialise**
B. There is **risk**
C. There is **high risk**.

This formal classifica7on of the level of risk to the rights and freedoms of the data subjects is essen7al as it is a key determinant of how the school should manage the breach.

6.5. When managing a personal data breach, the school is advised to pay par7cular a^en7on to relevant guidance issued on an ongoing basis by the *Data ProtecCon Commission* (DPC). For example, the DPC has listed the following criteria as important when evalua7ng the risk to the rights and freedoms of affected data subjects:

- the nature and circumstances of the breach;

---

[14] IT logs and audit trails (e.g. firewall, router and intrusion detec7on systems) can be a par7cularly important source of forensic informa7on following on a data security incident. The DPC may well enquire about these as part of its own review of a data breach incident.

[15] Although a personal data breach can present a source of risk to the school, the assessment required under GDPR Ar7cles 33, 34 is exclusively concerned with any <u>risk to the data subjects</u> affected by the breach. The *European Union Agency for Network and InformaCon Services* (ENISA) has published a methodology to help assess the severity of any breach, available at www.enisa.europa.eu/publica7ons/ dbn-severity

[16] The school must bear in mind that the poten7al impact of any data breach is not just loss of control over personal data. A breach can also result in other economic and social disadvantage including discrimina7on, iden7ty the], financial loss, damage to reputa7on, etc.

- the type of personal data affected (including whether it contains sensi7ve, or 'special category' personal data);
- the volume of personal data involved;
- the poten7al for the personal data to be used maliciously;
- the poten7al damage or harm to data subjects; and
- steps taken or the possibility to mi7gate the harm or damage. [17]

6.6. The DPC refers data controllers to relevant guidance issued at a European level. For example, the European
Data Protec7on Board (EDPB) recommends that any risk assessment should consider factors such as: [18]

- The type and circumstances of the breach (confiden7ality/availability/integrity)
- Special characteris7cs of the individual (e.g. a breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result).
- The nature, sensi7vity, and volume of personal data (e.g. breaches involving health data, iden7ty documents, or financial data such as credit card details, can all cause harm on their own, but if accessed together they could be used for iden7ty the]. A combina7on of personal data is typically more sensi7ve than a single piece of personal data).
- Ease of iden7fica7on of individuals (e.g. data protected by an appropriate level of pseudonymisa7on can reduce the likelihood of individuals being iden7fied; encryp7on can make data unintelligible to unauthorised persons without the decryp7on key).
- Severity of consequences for individual (e.g. whether personal data is in the hands of people whose inten7ons are possibly malicious, or alterna7vely, sent in error to a recipient who can be trusted not to read or access, may be factored into the risk assessment the controller carries out following the breach. Considera7on should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term).
- The number of affected individuals (Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data).

6.7. Where the school forms the opinion that there is "no likely risk" to the rights and freedoms of the data subjects, the reasons for that decision must be recorded. The *Data Security Breach Incident Report* form (Appendix 1) provides a template. It is important that any decision that there is no necessity to communicate with the DPC and/or affected data subjects, is jus7fied and documented within the records of the incident retained by the school, not least because this is a legal requirement under GDPR Ar7cle 33(5).[19]

---

[17] See "Assessing Risk" in *A PracCcal Guide to Personal Data Breach NoCficaCon's under the GDPR* (DPC Guidance Note, October 2019). h^ps://www.dataprotec7on.ie/sites/default/files/uploads/2019-10/Data%20Breach%20No7fica7on_Prac7cal%20Guidance_Oct19.pdf

[18] *Guidelines on Personal Data Breach NoCficaCon Under RegulaCon 2016/679 (WP250).*
hYps://ec.europa.eu/newsroom/arCcle29/ document.cfm?acCon=display&doc_id=49827

[19] "This means that the default posi7on for controllers is that all data breaches should be no7fied to the DPC, except for those where the controller has assessed the breach as being unlikely to present any risk to individuals and the controller can show

7. Mandatory NoPficaPons

7.1. **In the event of a personal data breach the school must** (inter alia):

i. No7fy the Data Protec7on Commission (DPC) without undue delay and not later than 72 hours unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

ii. Contact the data subjects without undue delay unless the personal data breach is unlikely to result in a high risk to the rights and freedoms of natural persons.

7.2. **ReporPng of incidents to the Data ProtecPon Commissioner (DPC):** All incidents in which personal data and sensi7ve personal data has been put at risk shall be reported to the Data Protec7on Commission without undue delay and where feasible, not later than 72 hours a]er having become aware of it unless it does not result in a risk to the rights and freedoms of data subjects.

7.3. While contact details for the Data Protec7on Commission are provided below, the recommended means of formally no7fying a personal data breach to the DPC, is to use the breach no7fica7on form available on the Commission's website.[20] Comple7ng and submiqng the breach report webform will generate the necessary acknowledgment and DPC case reference number.

DPC Contact details

Telephone:	0761 104 800
Lo Call Number:	1890 252 231
E-mail:	info@dataprotec7on.ie
Address:	Data Protec7on Commission, Canal House, Sta7on Road, Portarlington, R32 AP23, Co. Laois

7.4. GDPR Ar7cle 33(3) requires that, at a minimum, the following informa7on be provided to the DPC:

- ☐ nature of the personal data breach.
- ☐ categories (e.g. children, other vulnerable groups, people with disabili7es, employees, customers) and approximate number of data subjects affected.
- ☐ categories of personal data records (e.g. health data, educa7on records, social care informa7on, financial details, bank account numbers, passport numbers etc).
- ☐ approximate number of personal data records affected.
- ☐ likely consequences of the breach (e.g. loss of control of data, possible discrimina7on, iden7ty the], financial loss, physical risk etc).
- ☐ measures taken (or proposed) by the school to address the breach (including any measures to mi7gate its possible adverse effects).
- ☐ Contact point for more informa7on where appropriate

why they reached this conclusion. In any event, for all breaches — even those that are not no7fied to the DPC on the basis that they have been assessed as being unlikely to result in a risk — controllers must record at least the basic details of the breach, the assessment thereof, its effects, and the steps taken in response, as required by Ar7cle 33(5) GDPR." *Data ProtecCon Commission 2019 Annual Report* p35.

[20] DPC Breach No7fica7on Form h^ps://forms.dataprotec7on.ie/report-a-breach-of-personal-data

7.5. Important note: where the exact details of any of the above are not yet known, this shall not delay a 7mely breach no7fica7on to the DPC. Further informa7on can follow, when available: *"the informaCon may be provided in phases without undue further delay".*

7.6. Purpose of DPC no7fica7on:

(a) Advices: so that the school can obtain advices from the DPC, and to ensure that the school's decisions about no7fying (or deciding not to no7fy) affected data subjects can be jus7fied.

(b) Avoid an Administra7ve fine: Failure to no7fy the Data Protec7on Commission as required under the Data Protec7on Act 2018 may result in an administra7ve fine.

7.7. **NoPfying affected data subjects** Following the risk-assessment exercise (sec7on 6 of this procedure), if the personal data breach is deemed likely to result in a "high risk" to the rights and freedoms of natural persons, the school shall:

(a) Contact the individuals concerned (whether by phone/email etc) without undue delay.

(b) Advise that a data breach has occurred.

(c) Provide the data subjects with the detail outlined at 7.8 below.

(d) Where appropriate, provide specific advices (such as re-seqng passwords etc.) so that the data subjects can protect themselves from possible adverse consequences of the breach.

7.8. GDPR Ar7cle 34(2) requires that, at a minimum, the following informa7on be provided to the Data Subjects

- ☐ Descrip7on of any likely consequences of the personal data breach (e.g. iden7ty the], fraud, financial loss, threat to professional secrecy etc).
- ☐ Descrip7on of measures taken (or proposed) by the school to address the breach (including any measures to mi7gate its possible adverse effects).
- ☐ Contact point for more informa7on where appropriate

7.9. GDPR Ar7cle 34(3) states that a communica7on to the data subject shall not be required if any of the following condi7ons are met:

(a) the school has implemented appropriate technical and organisa7onal protec7on measures, and those measures render the personal data unintelligible to any person who is not authorised to access it;

(b) the school has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

(c) it would involve dispropor7onate effort. (In such a case, there shall instead be a public communica7on or similar measure whereby the data subjects are informed in an equally effec7ve manner.)

7.10. Where the DPC has reason to believe that the incident is being managed effec7vely by the school and that no further ac7on is needed to protect individual rights and freedoms, this may result in the case being closed. On the other hand, the DPC also has the op7on (and in some circumstances a statutory obliga7on) to take further ac7on in line with its powers under GDPR Ar7cle 58.[21]

[21] Under GDPR Ar7cle 58 the Data Protec7on Commission can, inter alia, (i) require the school to provide further informa7on or to compile a detailed report (ii) carry out a data protec7on audit (iii) carry out an on-site examina7on of school systems and procedures (iv) issue warnings or reprimands (v) impose an administra7ve fine (as set out in GDPR Ar7cle 83).

7.11. In addi7on to any sanc7on it might apply to the school (as controller), the DPC also has the power to prosecute individuals when it believes they have commi^ed offences under the Data Protec7on Act 2018, for example, where persons have knowingly or recklessly, disclosed personal data without the prior authority of the controller.[22]

8. EvaluaPon and Response

8.1. In the a]ermath of a data breach (or "near miss"), the school should carry out a post-incident review to ensure that the steps taken were appropriate and to iden7fy any areas that need improvement or ac7on.[23]

8.2. The extent of the post-incident review should be propor7onate to the seriousness of the incident and the level of risk associated with any data breach.

8.3. A post-incident review may involve considera7on of the following ques7ons:

- What ac7on needs to be taken to reduce the risk of future breaches and minimise their impact?
- Do policies, procedures or repor7ng lines need to be improved to increase the effec7veness of the school's response to a data breach?
- Are there weak points in security controls that need to be strengthened?
- Are people aware of, and adequately trained in, informa7on security measures?
- Is addi7onal investment required to reduce exposure and, if so, what are the resource implica7ons?

8.4. As any data breach incident file approaches closure, the various consulta7on channels (as set out earlier in sec7on 3 *CommunicaCons*) should be revisited to confirm that all appropriate ac7ons have been taken. The school should also confirm that its records of the personal data breach are comprehensive and sa7sfy the regulatory requirements.[24]

8.5. In certain circumstances the school may need to consider ini7a7ng ac7on under the appropriate school disciplinary procedure.[25]

---

[22] *Offences* are set out in the *Data ProtecCon Act 2018, Chapter 7*

[23] "Businesses and organisa7ons in control of personal data have an obliga7on to mi7gate against all poten7al future breaches. The DPC has observed an increase in the number of repeat breaches of a similar nature by a large number of companies. …..Data controllers can take simple steps to a^empt to mi7gate these risks such as running staff training and awareness programs; implemen7ng stringent password policies and mul7factor authen7ca7on for remote access; habitually upda7ng an7-virus and an7-malware so]ware; ensuring that email and web filtering environments are correctly configured; and, ensuring that all computer devices are regularly updated with manufacturers' so]ware and security patches." *Data ProtecCon Commission 2019 Annual Report* p35.

[24] GDPR Ar7cle 33(5): "The controller shall document any personal data breaches, comprising the facts rela7ng to the personal data breach, its effects and the remedial ac7on taken."

[25] For example, disciplinary ac7on may be required where an employee has received adequate training and guidance on data processing and security measures and ought reasonably to have been aware of the consequences for ac7ng in a manner contrary to school policy and procedures. Similarly, a student who causes a personal data breach by ac7ng in a manner that is at variance with the school's policies may also an7cipate a propor7onate sanc7on under the Code of Behaviour.

Appendix 1 - Data Security Breach Incident Report

1 Breach Timeline

Breach Timeline	
Do you know when the breach ini7ally occurred?	
When was incident discovered (specific 7me and date) and who reported the breach (data subject/employee/third party etc)?	
When did senior management become aware?	

2 About the Breach

DescripPon of how the breach occurred:
How would you categorise this breach?
(i) Impact on Data? (e.g. Destruc7on/Loss/Altera7on/Disclosure/Access/ Unavailability) (ii) Nature of breach? (e.g. Device/Paper Lost/Stolen/Inappropriate disposal/ Cyber-incident/ Unintended sharing/ Network security compromised etc.) (iii) Cause? (e.g. Employee/Contractor/External error/omission/inten7onal act etc.)

3 About the Breached Data

What categories of data subjects (e.g. students or other vulnerable groups, adult learners, parents/guardians, employees, board members, others etc.) were affected and/or potenPally affected by the breach?
Number of data subjects affected (actual/approximate/unknown)?

What idenPfying details (e.g. Name/DOB/Address/PPSN/Contact details/passport/Economic or Financial data/ LocaPon data/Other) relaPng to individuals were disclosed?
Were any special categories of data involved (racial or ethnic origin, PoliPcal opinions, Trade Union membership, Sex life data, Health data, GenePc data, Biometric data, Religious or philosophical beliefs)?
Number of data records affected (actual/approximate/unknown)?

4 Measures in place before the Breach and measures to respond to the Breach

Describe any relevant security/organisaPonal measures in place prior to the breach (passwords, encrypPon etc.) Have any deficiencies in these organisaPonal or technical measures been idenPfied as a result of this
breach?
Have any acPons/steps been taken to miPgate the risk to the data subject(s)? Describe measures taken (or proposed) by the school to address the breach. Can the personal informaPon be recovered?
Have you made any contact with external agencies e.g. Insurance Company, Gardaí, Legal advisors etc.? If YES, provide contact details and any advice provided.

Were any IT systems involved (e.g. email, website, MIS, apps)? Has any advice been obtained from IT provider/support? Is any addiPonal diagnosPc material available e.g. error messages, screen shots, log files, etc.?

5 Consequences and NoPficaPons

PotenPal consequences of the breach for individuals (e.g. loss of control over data, discriminaPon, idenPty thee, financial loss, reputaPonal damage etc)
How severe is the breach for affected individuals? Level of risk? None/Low/Medium/High/Severe. Note: Where you determine there is no risk, record <u>how</u> this was decided (including any consultaPon with Board).
Details of any contact with the DPC, including any formal breach noPficaPon(s) made in relaPon to this breach. (Copies of formal breach noPficaPons can be appended to this form).
Details of any contact made with data subjects, including any wrifen communicaPons(s) made in relaPon to this breach. Copies of formal wrifen communicaPons(s) can be appended to this form.

Signed:	
Your posiPon in the school:	

Date(s) of complePon:	
CONFIDENTIAL - THIS FORM HAS BEEN COMPLETED IN CONTEMPLATION OF LEGAL PROCEEDINGS	

Appendix 2 - Sources of Guidance on Data Security

The legal obliga7on to keep personal data secure applies to every data controller and data processor, regardless of size. The Data Protec7on Act 2018 and the General Data Protec7on Regula7on (GDPR) do not detail specific security measures that a data controller or data processor must have in place. The absence of detail on security measures within the legisla7on should be understood on the basis that the provision of such guidance within the legisla7on would run the risk of going out of date quite quickly due to changes in technology etc.

At the same 7me, the GDPR, in Ar7cles 25 and 32, does place an obliga7on on controllers and processors to implement data protec7on by design and by default and 'appropriate technical and organisa7onal measures' to ensure a level of security appropriate to the risk, taking into account:

- the state of the art;
- the costs of implementa7on;
- the nature, scope, context and purposes of processing; and
- the likelihood and severity of the risk to the rights and freedoms of individuals.

It goes on to suggest the following indica7ve list of appropriate measures:

- the pseudonymisa7on and encryp7on of personal data;
- the ability to ensure the ongoing confiden7ality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a 7mely manner in the event of a physical or technical incident; and
- a process for regularly tes7ng, assessing and evalua7ng the effec7ve of technical and organisa7onal measures for ensuring the security of the processing.

Data controllers and data processors are also obliged to ensure that their staff and other persons at the place of work are aware of security measures and comply with them.

DATA PROTECTION COMMISSION (DPC)

The DPC publishes guidance from 7me to 7me related to data security ma^ers. This guidance, though technical in nature, is usually accessible to a broad audience in that it is wri^en with the general reader in mind. Schools are advised to monitor the DPC website (www.dataprotec7on.ie) for relevant advice and to consider how it might apply within the school environment. Some examples of DPC guidance are listed below.

Guidance for Controllers on Data Security (updated February 2020)[26]

A set of general guidelines (12 pages) providing concrete advice for controllers in rela7on to issues such as:[27]

[26] h^ps://dataprotec7on.ie/en/guidance-landing/guidance-controllers-data-security

[27] In the event of a data breach it seems reasonable to an7cipate that the DPC may use a controller's compliance with its own guidance on data security as an indicator of "appropriate technical and organisa7on measures". Bearing this in mind, it would seem appropriate for school data controllers to carefully review this guidance document (and any other relevant advice from the DPC). As part of any internal review of data security measures, the school might ask their nominated IT service providers to validate that they have implemented systems that are aligned with this DPC advice.

- Access Controls
- Access Authen7ca7on (Passwords and Mul7-Factor Authen7ca7on)
- Automa7c Screen Savers
- Encryp7on
- An7-Virus So]ware
- Firewalls
- So]ware Patching
- Remote Access
- Wireless Networks
- Portable Devices
- Logs and Audit Trails
- Back-Up Systems
- Incident Response Plans
- Disposal of Equipment
- Physical Security
- The Human Factor
- Cer7fica7on

Guidance for OrganisaCons on Phishing and Social Engineering AYacks (October 2019)[28]

This guidance (6 pages) provides controllers with 7ps on how to spot phishing and social engineering a^acks, suggested approaches to mi7ga7ng risk, and a list of recommenda7ons on how to increase organisa7onal security.

- Tips to spot phishing or social engineering
- Approaches to mi7ga7ng the risk of a^acks
- Recommenda7ons to increase security against a^acks

Guidance Note: What should you be aware of online? Some common online risks (October 2019)[29]

Familiarity with this guidance (22 pages) will benefit both the individual and the organisa7on. It aims to build user awareness of online risks and suggest steps "to keep yourself and your personal data safe and to exercise choice and control in deciding how you engage online with social media and other online services". The second part of the guidance highlights a number of security-related issues, including:

- Password Reuse
- Security Ques7ons
- Phishing
- Unsecured Login Forms
- Domain Names – Spot Fake Sites

Guidance Note: Five Steps to Secure Cloud-based Environments (June 2019)[30]

Cloud-based environments offer many advantages; however, they also introduce a number of technical security risks which organisa7ons should be aware of, including data breaches, hijacking of accounts, and unauthorised access to personal data. This DPC guidance (3 pages) aims to assist organisa7ons understand their obliga7ons with regard to the security of personal data, and to mi7gate their risks when u7lising a cloud-based environment.

Guidance Note: General Portable Storage Device RecommendaCons (October 2019)[31]

Any organisa7on u7lising portable storage devices to store or transmit personal data should consider the par7cular risks associated with the use of such devices, such as loss or unauthorised access, and ensure that they have internal policies and technical measures which mi7gate these risks. This

guidance (3 pages) sets out recommenda7ons for organisa7ons to consider when planning their own internal policies on the use of portable storage devices.

Data Security Guidance for Microenterprises (July 2019)[32]

This guidance (10 pages) is targeted at microenterprises but as most of its recommenda7ons are equally applicable to an educa7onal seqng, it will be equally useful for schools engaged in a review of appropriate technical and organisa7onal security measures to safeguard the personal data they are processing. As well as addressing technical security, it also provides very useful checklists on physical security and organisa7onal security.

---

[28] h^ps://dataprotec7on.ie/en/guidance-landing/guidance-organisa7ons-phishing-and-social-engineering-a^acks

[29] h^ps://dataprotec7on.ie/en/guidance-landing/common-online-risks

[30] h^ps://dataprotec7on.ie/en/guidance-landing/five-steps-secure-cloud-based-environments

[31] h^ps://www.dataprotec7on.ie/en/guidance-landing/general-portable-storage-device-recommenda7ons

[32] h^ps://www.dataprotec7on.ie/en/guidance-landing/data-security-guidance-microenterprises

OTHER SOURCES

The **NaPonal Cyber Security Centre (Ireland)** was established a lead in the management of major cyber security incidents across government, and also to provide guidance and advice to ci7zens and businesses on major cyber security incidents. It has published a guide to cyber security for Irish business: *12 Steps to Cyber Security (October 2018)*.[28]

The **NaPonal Cyber Security Centre (UK)** has an extensive set of cybersecurity-related resources available on its website. These include support materials for public sector bodies[29] as well as specific guidance for school staff.[30] Those responsible for overseeing data security in schools may also find other NCSC resources to be of benefit, for example, its *Cyber Security: Small Business Guide*.[31]

ENISA, the European Union Agency for Cybersecurity, frequently publishes up to date guidance on cybersecurity, data protec7on and risk assessment available through its website.[32] For example, its *Guidelines for SMEs on the security of personal data processing*[33] explain how to implement a risk-based approach to data security. **Europol**, the European Union's law enforcement agency, also maintains some informa7on rela7ng to cybercrime on its website.[34]

---

[28] h^ps://www.ncsc.gov.ie/pdfs/Cybersecurity_12_steps.pdf

[29] h^ps://www.ncsc.gov.uk/sec7on/informa7on-for/public-sector

[30] h^ps://www.ncsc.gov.uk/informa7on/resources-for-schools

[31] h^ps://www.ncsc.gov.uk/files/cyber_security_small_business_guide_1.3..pdf

[32] h^ps://www.enisa.europa.eu/topics

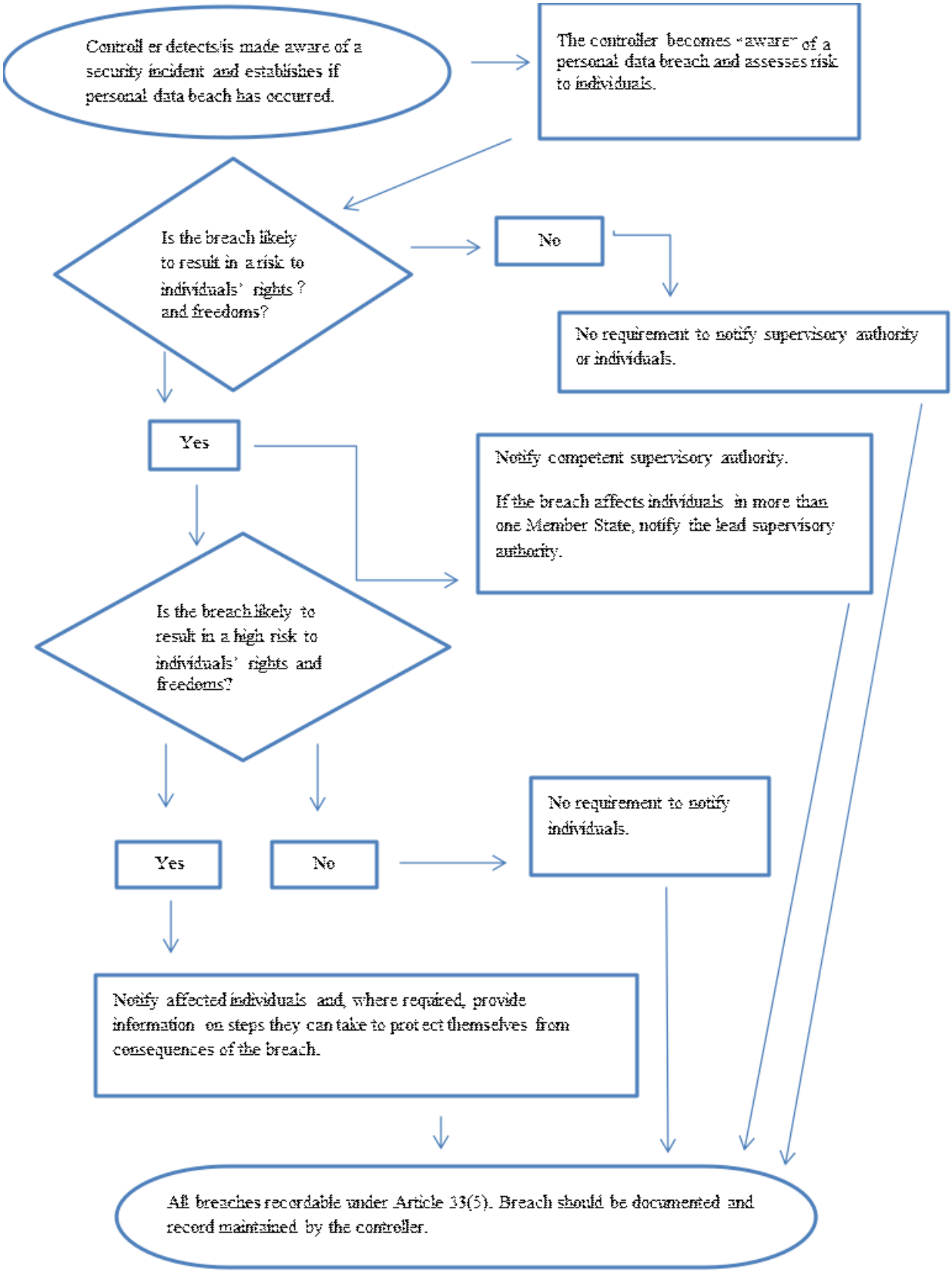
[33] h^ps://www.enisa.europa.eu/publica7ons/guidelines-for-smes-on-the-security-of-personal-data-processing

[34] h^ps://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

Professional Development Service for Teachers (PDST), a na7onal support service opera7ng under the aegis of the Department of Educa7on and Skills, supports the integra7on of ICT in teaching and learning within Irish primary and secondary schools. Where PDST shares guidance on IT security for schools this is likely to be available on the PDST Technology in Educa7on website.[35]

[35] h^ps://www.pds^echnologyineduca7on.ie/en/Technology/itsecurity/IT-Security.html

Appendix 3 - Flowchart showing regulatory noPficaPon requirements[36]



[36] This flowchart formed part of the *Guidelines on Personal data breach noCficaCon under RegulaCon 2016/679* adopted in 2018 by the **ArPcle 29 Data ProtecPon Working Party**, a body now recons7tuted as the **European Data ProtecPon Board**. h^ps://ec.europa.eu/ newsroom/ar7cle29/document.cfm?ac7on=display&doc_id=49827