Coláiste Cholmcille



Data Protection Policy

Contents

1. Introduction and Rationale 2
1.1 Mission Statement and Ethos 2
1.2 Rationale and Legal Compliance 2
1.3 Scope and Application 2

2. Definitions and Roles 3
2.1 Key Definitions 3
2.2 Data Protection Roles and Responsibilities 3

3. Core Data Protection Principles 4
3.1 Principle 1: Lawfulness, Fairness, and Transparency 4
3.2 Principle 2: Purpose Limitation 4
3.3 Principle 3: Data Minimisation and Accuracy 4
3.4 Principle 4: Storage Limitation 4
3.5 Principle 5: Integrity and Confidentiality (Security) 4
3.6 Principle 6: Accountability 4
3.7 Lawful Basis for Processing
3.8 CCTV Records 5

4. Rights of the Data Subject 5
4.1 The Right of Access (SAR) 5
4.2 Other Data Subject Rights 6
4.3 Processing Activities, Categories, and Purposes 7

5. Data Security & Breach Management 7
5.1 Data Breach Management 7
5.2 Device & Display Security 8
5.3 Breach Protocol & Reporting 8

6. Policy Implementation 8
6.1 Relationship to Other Policies and Sanctions 9
6.2 Data Processors and Data Sharing 9
6.3 Automated Processing and Artificial Intelligence (AI) 9

7. Third-Party Data Sharing 10

8. Ratification & Review 11
8.1 Implementation of Policy 11
8.2 Review of Policy 11

Appendix 1: Reference Sites and Resources 12

1. Introduction and Rationale

1.1 Mission Statement and Ethos

Coláiste Cholmcille is a community which respects the individual's rights and self-worth and aims to provide a happy and safe environment in which the individual may achieve her/his spiritual, academic and personal potential in order to develop all positive aspects of the individual and the community. Our Characteristic Spirit document states:

"The school is a caring and welcoming one, endeavouring to promote a culture of good relationships where people thrive and grow".

The core values of Coláiste Cholmcille are **respect, fairness and personal growth.** These values combine to provide and support an atmosphere which is conducive to excellence in teaching and learning. We endeavour to assist each student to reach their full potential in a calm, caring and creative environment.

In keeping with our Mission Statement, our **Code of Conduct** exists to promote a positive and productive teaching and learning atmosphere. Its aim is to ensure that each student passing through our care develops responsible attitudes underpinned by respect for self and others; students are required to take responsibility for their actions and consider the consequences for themselves and the school community.

1.2 Rationale and Legal Compliance

This policy outlines how Coláiste Cholmcille ensures compliance with data protection legislation, specifically the **EU General Data Protection Regulation (GDPR) 2016/679** and the **Data Protection Acts 1988–2018**. Coláiste Cholmcille is committed to protecting the fundamental rights and freedoms of individuals, particularly their right to privacy and the protection of their personal data.

1.3 Scope and Application

This policy applies to all **Personal Data** and **Special Category Data** (as defined in Section 2.1) processed by the school, regardless of whether the data is held in physical (paper) or electronic form. The policy applies to:

- The Board of Management (BoM)
- All teaching and non-teaching staff (Permanent, Temporary, and Substitutes)
- All students and their parents/guardians
- Others, including prospective students/staff and contractors/volunteers

2. Definitions and Roles

2.1 Key Definitions

Term	Definition in the Context of the College
Personal Data	Any information relating to an identified or identifiable person (Data Subject). This includes names, addresses, photos, student numbers, assessment grades, and financial information.
Special Category Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or data concerning health (e.g., medical conditions, SEN needs) or sexual orientation. This data requires extra protection.
Processing	Any operation performed on personal data, such as collection, recording, storage, consultation, transmission, or erasure.
Data Controller	The 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. **The Board of Management of Coláiste Cholmcille is the Data Controller.**
Data Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller.
Data Subject	The identified or identifiable natural person to whom the data relates (e.g., a student, a staff member, a parent).
Child	A person under the age of 18 years. Children are deemed as vulnerable under GDPR and merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data Protection Commission	The national supervisory authority responsible for monitoring the enforcing the data protection legislation within Ireland. The DPC is the organisation to which schools as data controllers must notify data breaches where there is risk involved.
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.

Transparancy	The school as Controller is obliged to act with transparency when processing personal data. This requires the communication of specific information to individuals in advance of any processing of their personal data.

2.2 Data Protection Roles and Responsibilities

- **Data Controller:** The **Board of Management (BoM)** of Coláiste Cholmcille holds the ultimate responsibility for data processing and compliance.
- **Principal:** The Principal is responsible for the day-to-day implementation of the policy, ensuring all staff are aware of their responsibilities.
- **Staff:** All staff members are responsible for processing data in accordance with the policy and immediately reporting any actual or suspected data breaches to the Principal.

3. Core Data Protection Principles

Coláiste Cholmcille adheres to the six core principles governing the processing of personal data:

3.1 Principle 1: Lawfulness, Fairness, and Transparency

Data is collected only where there is a lawful basis (e.g., legal obligation, performance of a contract, or explicit consent) and is processed fairly and transparently. Data Subjects are informed about how their data is used (via Privacy Notices).

3.2 Principle 2: Purpose Limitation

Data is collected only for specified, explicit, and legitimate purposes (e.g., education, welfare, administration) and is not processed in a manner that is incompatible with those purposes.

3.3 Principle 3: Data Minimisation and Accuracy

The data collected is adequate, relevant, and limited to what is necessary for the stated purpose. Coláiste Cholmcille takes every reasonable step to ensure that personal data is accurate and, where necessary, kept 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. However, records must not be altered or destroyed without proper authorisation.

3.4 Personal Data

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

A. Staff records:

(a) Categories of staff 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 under probation. These staff records ***may*** include:

• Name, address and contact details, PPS number

• 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 mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) 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.

• **Security**: Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. All Portable devices storing personal data (such as laptops) are encrypted and password protected. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

B. Student records:

(a) Categories of student 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 etc.) 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).

• Academic record – subjects studied, class assignments, examination results as recorded on official School reports

• Records of significant achievements

• Whether the student is repeating the Leaving Certificate

• Whether the student is exempt from studying Irish

• Records of disciplinary issues/investigations and/or sanctions imposed

• Garda vetting outcome record (where the student is engaged in work experience organised with or through the school/ETB which requires that they be Garda vetted)

• Other records e.g. records of any serious injuries/accidents etc. (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 mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) Purposes: The purposes for keeping student records are:

• to enable each student to develop to their 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, 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 requirements for their course,

• 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 third-level educational institutions and/or prospective employers

• In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the School will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.

(d) Security: Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) are encrypted and password protected. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

C. Board of management records:

(a) Categories of board of management data: These may include:

• 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 particular individuals.

(b) 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.

(d) Security: Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a

separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

D. Other records:

For example:

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive):

Creditors

(a) 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.

(b) 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.

(d) Security: Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

Charity tax-back forms

(a) Categories of data: the school may hold the following data in relation to donors who have made charitable donations to the school:

• Name

• address

• Telephone number

• PPS number

• Tax rate

• Signature and

• The gross amount of the donation.

(b) Purposes: Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parents name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the case of audit by the Revenue Commissioners.

(d) Security: Sensitive Personal Data is securely stored under lock and key in the case of manual records and protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

3.5 Principle 4: Storage Limitation

Data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, in line with the school's official Data Retention Schedule. **See Retention Policy**

This Data Protection Policy serves as the legal framework, while the Retention Policy acts as the technical index for the following record types:

Student Personal Data: Including PPSN, Mother's Birth Name, identification photographs, medical information, and Irish language exemptions.

Academic & Behavioural Records: Term reports, State Exam results, JCPA data, disciplinary files, and bullying investigation reports.

Welfare & SEN Records: Psychological assessments, IEPs, Child Protection records (retained indefinitely), and Guidance (Therapeutic vs. Educational) notes.

Administrative & Governance: Board of Management (BOM) Minutes (indefinite), Agendas, Attendance sheets, and Section 29 Appeal records.

Staff & Financial Records: Personnel files, Garda Vetting outcomes, and Revenue/Payroll documentation.

3.6 Principle 5: Integrity and Confidentiality (Security)

Personal data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, and against accidental loss, destruction, or damage, using appropriate technical or organizational measures. Data will be stored securely so that confidential information is protected.

3.7 Principle 6: Accountability

The Data Controller (BoM) is responsible for, and must be able to demonstrate compliance with, all the principles outlined above. All data processing activities are documented.

3.8 Lawful Basis for Processing

Coláiste Cholmcille must identify a lawful basis under GDPR Article 6 for every data processing activity. The primary lawful bases relied upon are:

- **Legal Obligation:** Processing necessary for compliance with a legal obligation to which the school is subject (e.g., DES returns, Child Protection legislation, employment law).
- **Public Interest:** Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school (i.e., operating a school, providing education).
- **Contract:** Processing necessary for the performance of a contract to which the data subject is party (e.g., staff employment contracts).

- **Legitimate Interests:** Processing necessary for the legitimate interests pursued by the school or a third party (e.g., CCTV operations, school security, fundraising), provided these interests are not overridden by the rights of the data subject.

Special Category Data: Processing data concerning health or other special categories of personal data (e.g., SEN needs, religious belief) requires an additional lawful condition under GDPR Article 9. The school relies on conditions such as substantial public interest and provision of health or social care.

3.9 CCTV Records

For the purposes of Safety and security of staff, students and visitors and to safeguard school property and equipment. CCTV is installed in Coláiste Cholmcille. Cameras are installed externally – outside the main entrance and around/outside of the building. Cameras are also installed internally on corridors. These CCTV systems may record images of staff, students and members of the public who visit the premises. The viewing station is in the Deputy Principal's Office. Access to images/recordings is restricted to the Principal and Deputy Principals of the school. Recordings are retained for 28 days, except if required for the investigation of an incident. Images/recordings may be viewed or made available to An Garda Síochána pursuant to Data Protection Acts legislation.

We use CCTV for the following purposes:

● to secure and protect the school's premises and assets;

● to deter crime and anti-social behaviour;

● to assist in the investigation, detection, and prosecution of offences;

● to monitor areas in which cash and/or goods are handled;

● to deter bullying and/or harassment;

● to maintain good order and ensure the school's Code of Behaviour is respected;

● to provide a safe environment for all staff and students;

● for the taking and defence of litigation;

● for verification purposes and for dispute-resolution, particularly in circumstances where there is a dispute as to facts and where the recordings may be capable of resolving that dispute.

4. Rights of the Data Subject

All Data Subjects (students, staff, parents) have specific rights regarding their personal data held by the school.

4.1 The Right of Access (SAR)

Data Subjects have the right to obtain confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data. Requests must be submitted in writing to the **Principal** and will be dealt with within the statutory timeframe (usually one calendar month).

4.2 Other Data Subject Rights

Data subjects (students, staff, and parents/guardians) also have the following rights:

- **Right to Rectification:** To have inaccurate data corrected or incomplete data completed without undue delay.
- **Right to Erasure ("Right to be Forgotten"):** To request the erasure of personal data where there is no compelling legal basis for its continued retention and processing.
- **Right to Restriction of Processing:** To restrict how their data is processed in certain circumstances, such as while accuracy is being verified.
- **Right to Data Portability:** To receive and transmit their personal data to another controller in a structured, commonly used, and machine-readable format (where processing is based on consent or contract).
- **Right to Object:** To object to processing based on grounds of public interest or the school's legitimate interests, unless the school demonstrates compelling legitimate grounds that override those interests.
- **Right not to be subject to automated decision making**: This right applies in specific circumstances (as set out in GDPR Article 22).
- **Right to Withdraw Consent:** In cases where Coláiste Cholmcille is relying on consent to process your data, you have the right to withdraw this at any time, and if you exercise this right, we will stop the relevant processing.

- **Limitations on Rights**: While Coláiste Cholmcille will always facilitate the exercise of your rights, it is recognised that they are not unconditional: Coláiste Cholmcille may need to give consideration to other obligations.

- **Right to Complain**

    - If you are concerned about how your personal data is being processed, then please address these concerns in the first instance to the Principal who is responsible for operational oversight of this policy.

    - A matter that is still unresolved may then be referred to the Data Controller (i.e., the Board of Management) by writing to the Chairperson c/o school.

    - Should you feel dissatisfied with how we have addressed a complaint or concern that you have raised, you have the right, as data subject, to bring the matter to the attention of the Irish Data Protection Commission.

5. Data Security & Breach Management

5.1 Physical and Digital Security

- **Physical Security:** Paper records are stored in locked, fire-resistant cabinets with restricted access.
- **Digital Security:** Use of encrypted school servers, role-based access in administrative software, and strong password protocols.

5.2 Device & Display Security

- **Hardware:** Laptops and desktops used for school business must be password/passcode protected and never left unattended while logged in.
- **Projection Screens:** Staff must ensure that no sensitive personal data (e.g., administrative software profiles, medical notes, or grades) is visible on projection screens in classrooms or common areas when students or unauthorised persons are present. Use of the "Freeze" or "Blank" screen function is mandatory when navigating between sensitive documents.

5.3 Breach Protocol & Reporting

- **Internal Reporting:** Any staff member who discovers or suspects a data breach (e.g., loss of a laptop, accidental sharing of an email list, or unauthorized access to a system) **must inform the Principal immediately**.
- **Statutory Reporting:** Any suspected data breach will be reported by the school to the Data Protection Commission (DPC) within 72 hours where required.

6. Policy Implementation

6.1 Relationship to Other Policies and Sanctions

This policy is the cornerstone of our compliance framework and must be read alongside the following:

- **Data Retention Policy:** Providing the extensive list of data categories and disposal timelines.
- **Admissions Policy:** Regarding the processing of applicant data and waiting lists.
- **Anti-Bullying Policy & Code of Behaviour:** Regarding the creation and retention of disciplinary and investigation records.
- **Acceptable Use Policy (AUP) & AI Policy:** Regarding the digital footprint and data generated through school systems and artificial intelligence tools.
- **Child Protection Policy:** Regarding the permanent retention of safeguarding records.

6.2 Data Processors and Data Sharing

Coláiste Cholmcille will, at times, share data with third-party Data Controllers (e.g., Department of Education and Skills, SEC, TUSLA) as required by legal obligations. When engaging third-party **Data Processors** (e.g., cloud-based systems, IT providers, software vendors) who process personal data on the school's behalf, the school will ensure:

- The processor provides **sufficient guarantees** regarding technical and organisational security measures.
- A formal, signed **Data Processing Agreement (DPA)** is always put in place to govern the processing activities and ensure compliance with GDPR.

6.3 Automated Processing and Artificial Intelligence (AI)

The school recognises that data processing may increasingly involve automated systems and Artificial Intelligence (AI) tools.

- **Principle Adherence:** All use of AI and automated data processing must fully adhere to the six core GDPR principles.
- **Automated Decision-Making (Article 22):** The school shall not use fully automated systems to make decisions that significantly affect a data subject (e.g., disciplinary action, assessment outcomes) without meaningful human review, in line with the data subject's Right not to be subject to automated decision-making.
- **DPIA for AI:** A **Data Protection Impact Assessment (DPIA)** is mandatory before implementing any new AI system or process that involves high-risk activities, such as large-scale profiling, monitoring, or biometric data processing of students or staff.
- **Security and Third-Party Tools:** Staff and students are **prohibited** from inputting personal data, sensitive school information, or confidential records into generic, third-party generative AI tools (e.g., ChatGPT, Gemini, etc.) unless a formal Data Processing Agreement (DPA) is in place with the vendor and approved by the Data Controller.

7. Third-Party Data Sharing

The school sharing of data is conducted strictly under legal obligation or with explicit consent. Our data mapping identifies the following key third-party recipients:

- **Statutory Bodies:** Department of Education (DES), Revenue Commissioners, TUSLA, NCSE, and the State Examinations Commission.
- **Financial & Administrative Partners:** Bank for school accounts, and providers for staff deductions (Trade Unions, VHI/Laya, AVC providers).
- **Systems Providers:** Cloud-based management systems and the Department's **P-POD** (Post Primary Online Database) system.

8. Ratification and Review

8.1 Implementation of Policy

Coláiste Cholmcille's Data Protection Policy has been ratified by the Board of Management and formally adopted on the .

Signature…….. Date……

Chairperson of BoM

Signature…… Date……

Principal

8.2 Review of Policy

The school will monitor / review on a regular basis, and evaluate the policy and all related work and procedures to ensure legal compliance and the maintenance of best practices.

Date for Review: ……..

Appendix 1: Reference Sites and Resources

This list is provided for staff and parents/guardians to access reliable, official information on Data Protection and GDPR.

Reference	URL
Data Protection Act 2018	http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html
General Data Protection Regulation (GDPR official text) 2016	https://eur-lex.europa.eu/eli/reg/2016/679/oj
General Data Protection Regulation (GDPR unofficial web version) 2016	https://gdpr-info.eu/
GDPR for Schools website	https://gdpr4schools.ie/

Data Protection for Schools	http://dataprotectionschools.ie/en/
Irish Data Protection Commission (DPC)	https://www.dataprotection.ie/
Data Breach Report (DPC link)	https://forms.dataprotection.ie/report-a-breach-of-personal-data
European Data Protection Board (EDPB)	https://edpb.europa.eu/
EDPB Guidelines, Recommendations and Best Practices on GDPR	https://edpb.europa.eu/our-work-tools/general-guidance/gdprguidelines-recommendations-best-practices_en
DES Data Protection Page	https://www.education.ie/en/The-Department/Data-Protection/Information.html
PDST Technology in Education	https://www.pdsttechnologyineducation.ie
Cyber Security Centre (Ireland)	https://www.ncsc.gov.ie/