Westport Educate Together National School

Data Protection Policy

Created Date	March 2020
Created By	Niall Quinn (Principal)
Signed by Principal	
Version	V1_28April2020
Approved by Chairperson name	Linda McNulty
Approved by Chairperson signature	
Approved by Board Date	
Date of next review	September 2020

Contents

1. Data Protection Principles: 3
2. Purpose of the policy: 4
3. Definition of Data Protection Terms: 4
4. Rationale: 5
5. Other Legal Obligations: 5
6. Relationship to the Characteristic Spirit of the School: 6
7. Personal Data: 7
    7.1 Staff records 7
    7.2 Student records 8
    7.3 Board of Management records 9
    7.4 Other records 9
    7.5 CCTV images/recordings 10
    7.6 Test results 10
    7.7 Links to other policies and curriculum delivery 11
    7.8 Processing in line with data subject's rights 11
    7.9 Dealing with a data access request 11
    7.10 Providing information over the phone 12
8. Ratification and Communication: 12
9. Guidelines for taking and using images of pupils in schools: 13
    9.1 Contexts and purpose of images 13
    9.2 What is considered good practice when schools take photos of students? 14
    9.3 What is 'informed consent'?? 14
    9.4 Images taken by pupils 15
    9.6 Publishing images of pupils on websites 16
    9.7 Other people taking photos of children at school events 17
10. Records retention schedule: 17
    10.1 Student records 18
    10.2 Staff records: 20
    10.3 Board of Management records 26
    10.4 Government returns: 28
11. Personal Data Security Breach Code of Practice Form: 28

1. Data Protection Principles:

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

The policy applies to all school staff, the board of management, parents/guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

The school 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 school is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 which can be summarised as follows:

- **Obtain and process *Personal Data* fairly**: Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. 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 Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.

- **Keep it only for one or more specified and explicit lawful purposes**: The School will inform individuals of the reasons they collect their data and will inform individuals of 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.

- **Process it only in ways compatible with the purposes for which it was given initially**: 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.

- **Keep *Personal Data* safe and secure**: Only those with a genuine reason for doing so may gain access to the information. 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.

- **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. The principal may delegate such updates/amendments to another member of staff. However, 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.

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

- **Retain it 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 and Sensitive 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 Appendix 1: Records Retention Schedule)***

- **Provide a copy of their *personal data* to any individual, on request**: Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

2. Purpose of the policy:

The Data Protection Acts 1988 and 2003 apply to the keeping and processing of *Personal Data*, both in manual and electronic form. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, students and their parents/guardians how their data will be treated.

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.

3. 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:
Data means information in a form that can be processed. It includes both *automated data* (e.g. electronic data) and *manual data*. *Automated data* means any information on computer, or information recorded with the intention that it be *processed* by computer. *Manual data* means information that is kept/recorded as part of a *relevant filing system* or with the intention that it form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily, quickly and easily accessible.

Personal Data means data relating to 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 i.e. the school.

Sensitive Personal Data refers to *Personal Data* regarding a person's:

- racial or ethnic origin, political opinions or religious or philosophical beliefs
- membership of a trade union
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence or
- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

Data Controller for the purpose of this policy is the board of management, Westport ETNS National School.

4. 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 and 2003.

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. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

The school takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the principal and board of management to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and board of management.

5. 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

- 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, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational history or monitoring their educational progress in order to ascertain how best they may be assisted in availing of educational opportunities or in developing their educational potential; 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 ("SENOs")) 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 schools are not currently subject to freedom of information legislation, 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 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: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

6. Relationship to the Characteristic Spirit of the School:

Westport Educate Together seeks to:

- enable each student to develop to 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 Acts.

7. Personal Data:

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

7.1 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.

(c) **Location**: Staff records are stored in a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** Records are kept manually (in a personal file within a *relevant filing system*), in a secure, locked filing cabinet that only personnel who are authorised to use the data can access.

7.2 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 – Standardised test results as recorded on official School reports
- Records of significant achievements
- Whether the student is repeating a class level
- 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 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. Such records are taken and used in accordance with the school's "Guidance for Taking and Using Images of Pupils in Schools" (see template)
- 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

(c) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access and online on a password protected database run by the DES. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** Records are kept manually (in a personal file within a *relevant filing system*), in a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Pupil data is also stored on the DES Primary online database (POD) and on the Aladdin portal. Access to this data base is through a password protected network.

7.3 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.

(c) **Location**: In a secure, locked filing cabinet and that only personnel who are authorised to use the data can access it. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** Records are kept manually in a BOM file within a *relevant filing system*. A password protected computer record is also kept of minutes of the BOM meetings.

7.4 Other records

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
- 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.

(c) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(d) **Security:** Records are kept manually (in a personal file within a *relevant filing system*), in a secure, locked filing cabinet that only personnel who are authorised to use the data can access.

7.5 CCTV images/recordings

(a) **Categories**: CCTV is installed in some schools, externally i.e. perimeter walls/fencing and internally as detailed in the CCTV Policy. These CCTV systems may record images of staff, students and members of the public who visit the premises.

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

(c) **Location**: Cameras are located externally as detailed in the CCTV Policy. Recording equipment is located in the store room located off the office.

(d) **Security**: Access to images/recordings is restricted to the principal & deputy principal. 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 section 8 Data Protection Acts 1988 and 2003.

7.6 Test results

(a) **Categories**: The school will hold data comprising test results in respect of its students. These include infant screening tests, standardised test results and the results of diagnostic assessments.

(b) **Purposes**: The main purpose for which these results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about their progress. The data may also be aggregated for statistical/reporting purposes, such as to compile results for School Self Evaluation. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.

(c) **Security:** Records are kept manually in a BOM file within a *relevant filing system*. A password protected database is also kept comprising of annual standardised test results.

7.7 Links to other policies and curriculum delivery

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 Good Behaviour
- Mobile Phone Policy
- Enrolment Policy
- CCTV Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE Policy

7.8 Processing in line with data subject's rights

Data in this school will be processed in line with the data subjects' rights.

Data subjects have a right to:

(a) Request access to any data held about them by a data controller
(b) Prevent the processing of their data for direct-marketing purposes
(c) Ask to have inaccurate data amended
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

7.9 Dealing with a data access request

Section 3 access request

Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether the school holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 21 days.

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

Section 4 access request

Individuals are entitled to a copy of their personal data on written request.

- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- Request must be responded to within 40 days
- Fee may apply but cannot exceed €6.35
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

7.10 Providing information over the phone

In our school, any 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:

- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.

Implementation Arrangements, Roles and Responsibilities
In our school the board of management is the data controller and the principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to Personal Data are familiar with their data protection responsibilities. The following personnel have responsibility for implementing the Data Protection Policy:

Name	Responsibility
Board of management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality

8. Ratification and Communication:

This data protection policy was ratified by the BOM in April 2020. It was then circulated to all parents/guardians. All staff members are familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. This policy will be

read through at the first staff meeting of each school year to remind staff members of their roles in relation to data protection. All concerned will be made aware of any changes implied in recording information on students, staff and others in the school community.

Parents/guardians and students will be informed of the Data Protection Policy from the time of enrolment of the student e.g. by including the Data Protection Policy on the school website.

Monitoring the Implementation of the Policy
The implementation of the policy shall be monitored by the principal and a sub-committee of the board of management.
At least one annual report will be issued to the board of management to confirm that the actions/measures set down under the policy are being implemented.

Review and Evaluation of the Policy
The policy will be reviewed and evaluated annually. On-going review and evaluation should take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or the NEWB), 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.

This policy adopted by Board of Management on 28th April 2020.

Signed: _____
Linda McNulty (Chairperson)

Signed: _____
Niall Quinn (Principal)

9. Guidelines for taking and using images of pupils in schools:

9.1 Contexts and purpose of images

Source: Arts Council Guidelines for taking and using images of children and young people in the arts sector.
Photographs and video images can be made in a variety of contexts and settings - public, private, and semi-private - and for a range of purposes which might include:
Documenting and recording or illustrating work processes and events.

- Artistic work – created by pupils individually or collectively.
- Reporting to specific interest group such as evaluators, funding agencies, sponsors and/or the general public.
- Promotional work.

9.2 What is considered good practice when schools take photos of students?

- Recorded images should only be made, kept, and used where there is a valid reason for doing this.
- Recording of images should be adequately supervised as would any other activity.
- Pupils and their parent/guardian should be informed in advance if and when images will be taken, and their written consent should be sought for image retention and use. The school must spell this out very clearly so that the parent/guardian understands what processing will be involved. This process is known as 'informed consent'.
- Pupils and their parent/guardian should be informed as to how and where images will be used.
- Images should only be used for the purpose(s) agreed.
- Images should only be used in the intended context and should not be used out of context.
- In general, individual pupils should not be identified, with the exception being where they are being publicly acknowledged (e.g., an award, performance, achievement) for which informed consent has been given in writing by a parent/guardian.
- For publicity purposes, group photographs are preferable to individual ones. Where the "publicity purpose" includes a school website, prospectus, brochure, yearbook, newsletter etc, schools must be aware that parental/guardian consent can be withdrawn at any time for the use of their child's images, so it must be possible for the school to take down/delete the relevant images if the parental/guardian consent is withdrawn.
- Ensure all pupils are appropriately dressed.
- Ensure that images do not contribute to or expose children to embarrassment, distress or upset.
- Use images that represent the diversity of pupils participating in any given activity or setting.
- Do not use images of pupils who are considered vulnerable or whose identity may require protection.
- Permission to take and use images of pupils can be requested as part of the school enrolment process. However schools should note that a parent/guardian has the right to withdraw this consent at any time.
- Refusal of consent should not in any way limit pupil's participation in school activities.
- Where images are kept for future use, relevant names, dates and other contextual information should be stored with them as well as copies of the signed consent for their usage.
- Images should be carefully and securely stored in accordance security and storage and with the consent attached or cross referenced.
- Images should only be passed to third parties for their use where this has been explicitly agreed in writing as part of the consent process. A parent/guardian should have to "opt-in" to elect to have their child's images transferred to third parties (rather than to "opt-out").

9.3 What is 'informed consent'??

Informed consent is a process whereby participants are informed and asked for their permission or agreement prior to taking photographs or recording images. Individuals should be informed of:

- the purpose(s) the image will be used for, and

- the people/bodies to whom it might be transferred.

The individual should be asked for their prior written consent. Where images may be used for a variety of purposes (e.g., documenting, promoting or celebrating through press overage, websites, prospectuses etc.), consent for each purpose and/or in a variety of settings (e.g., reports, public media, or websites) should be obtained on an "opt-in" basis.

For example:

We would like to take photos/digital images of your child and use them for the following purposes. Do you give your consent as parent/guardian for us to do each of the following:

Tick box if "yes" you agree with these uses

Use on our school website? ☐

Use in our school brochure and yearbook? ☐

Use in our yearly school report? ☐

Retain in our school archives? ☐

We would also like to transfer photos//digital images of your child to the local newspaper, [insert name of local newspaper] for use in a piece celebrating the [insert school event, e.g. opening of new school building]. Do you give your consent for us to transfer these images to [name of newspaper] for these purposes?

Tick box if "yes" you permit this transfer

Yes, I give my consent ☐

Signed: _____

Parent/Guardian or Student (where over 18 years)

As a 'child' is anyone under the age of 18 years, consent of a parent/guardian is required. For further information and guidance, see Age of Consent for Processing.

In addition, the individual should be given any other information required to ensure fairness and transparency. For example, individuals should be informed if the image will be passed on or made available to a third party, used for school promotional purposes or displayed on the school website. This should be clearly explained as part of the process of informed consent, and their consent should be obtained (preferably on an "opt-in" basis) for each of these intended uses. If this is not done, or if consent is refused, then images should not be passed on to third parties or put to any use not agreed. Informed consent includes being given the opportunity to withdraw consent which had been previously given, if desired. Their right to withdraw any consent previously given must be free of charge, and not result in the data subject suffering any detriment.

It is recommended that schools seek consent at the time of enrolment to cover the period that the pupil will spend at the school. A copy of the school's Data Protection Policy should also be given to the student's parent/guardian on the enrolment of their child to the school, and the enrolment form should ask for the parent/guardian to sign their consent to their child's data (and their data) being processed in accordance with that Data Protection Policy for the duration of their child's time in the school. The enrolment form should also incorporate a consent form for contacting the parents/guardian, and also for the taking and use of the student's photos during the child's time at the school. Parents/guardians should be advised to inform the school if circumstances change and they no longer wish their child's image to be taken and retained.

9.4 Images taken by pupils

Images taken by pupils

It should be noted that Data Protection law does not apply to personal data kept by an individual for personal or family affairs, or for recreational purposes. Accordingly, photos and video clips taken by students of other students will not come within the Data Protection Acts. However, schools

understand that as part maintaining a nurturing school environment which is respectful and safe, they have a role to play in ensuring that students develop a respectful and appropriate attitude to the internet, social media, and their mobile devices. In circumstances where children or young people take photographs or video clips of other pupils, and other individuals, for their own use, similar ground rules should be agreed in partnership with parents/guardians.

- Images should only be taken with the knowledge and consent of participants.
- No images should be taken which could give rise to embarrassment or distress.

To this end it is advisable to set a clear policy for the use of mobile phones in school. as most now Schools are advised to put in place a Mobile Phone Policy and ensure that this dovetails with the school's Code of Behaviour.

9.5 Copyright

Ownership of copyright rests with the artist/photographer (or their employer). Images are not owned by the individual(s) whose image is recorded. Permission to use images owned by a photographer or agency is by prior agreement with the copyright holder.

9.6 Publishing images of pupils on websites

Schools need to develop a policy about the use of images of children on their websites. The internet is a public, accessible and largely unregulated media. Decisions to post information, including images, on websites should take account of this. Photographs set in a particular context (e.g., a school event) in an identified location (i.e. the school) reveal a substantial amount of information through which children may be identified. For example, images accompanied by personal information - (name) is a pupil of (school) and recently took part in xxx) - could be used by an individual to learn more about a child or young person, and used to form a relationship with them or engage in a process of 'grooming' them for abuse. A school needs to make decisions about the type of images that represent the school and its activities appropriately, and to ensure parents/guardians support the policy. The informed, explicit written consent of each parent/guardian should be obtained before their child's photo is uploaded to the school website.
Parents/guardians and students aged over 18 years have the right to insist that the school takes down any photo(s) containing an image of them or their child at any time, and this right must be fully respected. Where such a request is made by a parent/guardian or by a student aged over 18 years, every effort should be made to take the photo(s) down as soon as possible.
In general, when assessing risk, the most important factor is the potential of inappropriate use of the images. Schools should take the following steps to reduce the potential for misuse:

- Avoid using pupils' names (first name or surname) in photograph captions.
- Ensure that the school has written parental/guardian permission to use an image of their child where the child is under 18 years. For further information and guidance, see Age of Consent for Processing.
- Only use images of pupils in suitable dress to reduce the risk of inappropriate use.
- Certain activities present a much greater risk of potential misuse. It is preferable to use images that depict an activity or group context, rather than a particular pupil.
- Consider the age of pupils when deciding what is appropriate.
- Develop a procedure for reporting the use of inappropriate content or images to help reduce the risks to children and young people. (See:Office of Internet Safety www.internetsafety.ie).

9.7 Other people taking photos of children at school events

Schools are often asked whether parents can take photographs or make video recordings of school events e.g. nativity plays, musicals, and other school events. Parents are there at the invitation of the school, and it is up to the school to decide if it wishes to allow videos or photographs to be taken by parents during the event. However, schools should understand that taking photos or videos for purely personal, family, or recreational purposes does not come under the Data Protection Acts. Accordingly, the Data Protection Acts do not apply. However, individuals have a Constitutional unremunerated right to privacy**, therefore it would be prudent to state at the beginning of the school event (or in promotional material advertising the school event such as a school newsletter telling parents about the nativity play) that parents/guardians are permitted to take photographs or videos for private, personal use only, and that they must not be uploaded to any website to be viewed by others (e.g. Facebook).**

Where the student is under 18 years, the student's parent/guardian must be asked to give consent for school to process images of that child for the schools promotional use, e.g. publicising an event, sending photos to the press, putting photos on the school website, transmitting photos over the internet to the press, and use in school newsletters/brochures. For further information and guidance in relation to who gives consent, see Age of Consent for Processing. Where the student is over 18 years (and that student is not suffering under a mental disability or medical condition which may impair their capacity to give their consent) only the student's consent need be obtained for this processing. This may be done at the time of enrolment via the enrolment form data protection statement or for each event as the school deems necessary. Parents/guardians have the right to insist that the school takes down or removes any photo(s) containing an image of their child at any time, and this right must be fully respected. Where such a request is made by a parent/guardian or by a student (aged 18 years or older), every effort should be made to take the photo(s) down/remove the photo as soon as possible.

10. Records retention schedule:

Schools as *data controllers* must be clear about the length of time for which personal data will be kept and the reasons why the information is being retained. In determining appropriate retention periods, regard must be had for any statutory obligations imposed on a data controller. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner. It may also be anonymised to remove any personal data. Anonymisation must be irrevocable; removing names and addresses may not necessarily be sufficient.

In order to comply with this legal requirement, Westport ETNS has assigned specific responsibility and introduced procedures for ensuring that files are purged regularly and securely and that personal data is not retained any longer than is necessary. All records will be periodically reviewed in light of experience and any legal or other relevant indications.

IMPORTANT: In all cases, schools should be aware that where proceedings have been initiated, are in progress, or are reasonably foreseeable (although have not yet been taken against the school/board of management/an officer or employee of the school (which may include a volunteer)), all records relating to the individuals and incidents concerned should be preserved and should under no circumstances be deleted, destroyed or purged. The records may be of great assistance to the school in defending claims made in later years.

WARNING: In general, the limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim and the Statue of Limitations may be different in every case. In all cases where reference is made to "18 years" being the date upon which the relevant period set out in the Statute of Limitations commences for the purposes of litigation, the school must be aware that in some situations (such as the case of a student with special educational needs, or where the claim relates to child sexual abuse, or where the student has not become aware of the damage which they have suffered, and in some other circumstances), the Statute of Limitations **may not begin to run when the student reaches 18 years of age and specific legal advice should be sought by schools on a case-by-case basis.** In all cases where retention periods have been recommended with reference to the relevant statutory period in which an individual can make a claim, these time-frames may not apply where there has been misrepresentation, deception or fraud on the part of the respondent/defendant. In such a circumstance, the school should be aware that the claim could arise many years after the incident complained of and the courts/tribunals/employment fora may not consider the complainant to be "out of time" to make their claim.

10.1 Student records

Student Records	Period Held	Comments	Final disposition
Registers/ Roll books	Indefinitely	Indefinitely. Archive when class leaves + 2 years	N/A

Records relating to pupils/students	Primary	Comments	Confidential shredding
Enrolment Forms	Student reaching 18 years + 7 years	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Student transfer forms (Applies from primary to primary; from one second-level school to another)	If a form is used- Student reaching 18 years + 7 years	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Disciplinary notes	Never destroy	Never destroy	N/A
Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results)	Student reaching 18 years + 7 years	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school).	Confidential shredding
End of term/year reports	Student reaching 18 years + 7 years	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Records of school tours/trips, including permission slips, itinerary reports	Never destroy	Never destroy	N/A
Scholarship applications e.g. Gaeltacht, book rental scheme	Student reaching 18 years + 7 years	18 is age of majority plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Garda vetting form & outcome - **STUDENTS**	**N/A as primary schools pupils**	Record of outcome retained for 12 months. School to retain the reference	Confidential shredding

	will not be undergoing vetting	number and date of disclosure on file, which can be checked with An Garda Siochana in the future.	

Sensitive Personal Data Students	**Primary**	**Comments**	**Final disposition**
Psychological assessments	Indefinitely	Never destroy	N/A - Never destroy
Special Education Needs' files, reviews, correspondence and Individual Education Plans	Indefinitely	Never destroy	N/A
Accident reports	Indefinitely	Never destroy	N/A
Child protection records	Indefinitely	Never destroy	N/A
Section 29 appeal records	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Enrolment/transfer forms where child is not enrolled or refused enrolment	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Records of complaints made by parents/ guardians	Depends entirely on the nature of the complaint.	Depends entirely on the nature of the complaint. If it is child-safeguarding, a complaint relating to teacher-handling, or an accident, then retain indefinitely. Never destroy. If it is a complaint of a more mundane nature (e.g. misspelling of child's name, parent not being contacted to be informed of parent-teacher meeting) or other minor matter, then student reaching 18 years + 7 years (6 years in which to take a claim, and 1 year for proceedings to be served on school)	Confidential shredding or N/A, depending on the nature of the records.

10.2 Staff records:

Staff Records	Primary	Comments	Final disposition
Recruitment process Note: these suggested retention periods apply to unsuccessful candidates only. They do NOT apply to successful candidates, or candidates who are/were also employees already within your school applying for another post/position. For successful candidates, or candidates who are/were also employees already within your school applying for another post/position, see retention periods set out below.	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding
Applications & CVs of candidates called for interview	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding
Database of applications	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding
Selection criteria	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding
Applications of candidates not shortlisted	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding
Unsolicited applications for jobs	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding
Candidates shortlisted but unsuccessful at interview	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding

Candidates shortlisted and are successful but do not accept offer	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding
Interview board marking scheme & board notes	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding
Panel recommendation by interview board	✓	18 months from close of competition: 12 months from close of competition plus 6 months for the Equality Tribunal to inform the school that a claim is being taken.	Confidential shredding

Staff personnel files (whilst in employment)	**Primary**	**Comments**	**Final disposition**
e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, records of staff training etc.		Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding. Retain an anonymised sample for archival purposes.
Application &/CV	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Qualifications	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
References	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding

Interview: database of applications (the section which relates to the employee only)	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Selection criteria	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Interview board marking scheme & board notes	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Panel recommendation by interview board	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Recruitment medical	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Job specification/ description	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Contract/Conditions of employment	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Probation letters/forms	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding

POR applications and correspondence (whether successful or not)	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Leave of absence applications		Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Job share	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Career Break	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Maternity leave	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding
Paternity leave	✓	Retain for 2 years following retirement/resignation or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).	Confidential shredding
Parental leave	✓	Must be kept for 8 years - Parental Leave Act 1998 Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater).	Confidential shredding

		There is a statutory requirement to retain for 8 years.	
Force Majeure leave	✓	Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years.	Confidential shredding
Carers leave	✓	Must be kept for 8 years - Carer's Leave Act 2001 Retain for 8 years or the duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the greater). There is a statutory requirement to retain for 8 years	Confidential shredding
Working Time Act (attendance hours, holidays, breaks)	✓	Retain for duration of employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school). There is a statutory requirement to retain for 3 years	Confidential shredding
Allegations/complaints	✓	Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). **Please note** the relevant DES Circular re Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.	ETB one doesn't have a time period advised
Grievance and Disciplinary records	✓	Retain for duration of employment plus 7 years (6 years to take a claim, plus 1 year for proceedings to be served). **Please note** the relevant DES Circular re	

		Disciplinary Procedures in relation to the period of time for which a warning remains "active" on an employee's record.	

Occupational Health Records	**Primary**	**Comments**	**Confidential shredding**
Sickness absence records/certificates	✓	Re sick leave scheme (1 in 4 rule) ref DES C/L 0060/2010 Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.	Confidential shredding Or do not destroy.
Pre-employment medical assessment	✓	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.	Confidential shredding Or do not destroy?
Occupational health referral	✓	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.	Confidential shredding Or Do not destroy.
Correspondence re retirement on ill-health grounds	✓	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.	Confidential shredding Or Do not destroy.
Accident/injury at work reports	✓	Retain for 10 years, or the duration of the employment plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), whichever is the greater (unless sickness absence relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy).	Confidential shredding
Medical assessments or referrals	✓	Retain for 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school), unless Medmark assessment relates to an accident/ injury/ incident sustained in relation to or in connection with the individual's duties within the school, in which case, do not destroy.	Confidential shredding Or Do not destroy.
Sick leave records (sick benefit forms)	✓	In case of audit/refunds, Current year plus 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school)	Confidential shredding

Superannuation /Pension /Retirement records	Primary	Comments	Final disposition
Records of previous service (incl. correspondence with previous employers)	✓	DES advise that these should be kept indefinitely.	
Pension calculation	✓	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)	Confidential shredding
Pension increases (notification to Co. Co.)	✓	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)	Confidential shredding
Salary claim forms	✓	Duration of employment + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) or for the life of employee/former employee plus + 7 years (6 years in which to take a claim against the school, plus 1 year for proceedings to be served on the school) (whichever is the longer)	Confidential shredding

10.3 Board of Management records

Board of Management Records	Primary	Comments	Final disposition
Board agenda and minutes	✓	Indefinitely. These should be stored securely on school property	N/A
School closure	✓	On school closure, records should be transferred as per Records Retention in the event of school closure/amalgamation. A decommissioning exercise should take place with respect to archiving and recording data.	
Other school based reports/minutes	**Primary**	**Comments**	**Final disposition**
CCTV recordings	✓	28 days in the normal course, but longer on a case-by-case basis e.g. where recordings/images are requested by An Garda Síochána as part of an investigation or where the records /images capture issues such as damage/vandalism to school property and where the images/recordings are retained to investigate those issues.	Safe/secure deletion.

Principal's monthly report including staff absences	✓	Indefinitely. Administrative log and does not relate to any one employee in particular: the monthly reports are not structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. Not a "relevant filing system".	N/A
Financial Records	**Primary**	**Comments**	**Final disposition**
Audited Accounts	✓	Indefinitely	n/a
Payroll and taxation	✓	Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained **indefinitely** within the school. These records can be kept either on a manual or computer system.	
Invoices/back-up records/receipts	✓	Retain for 7 years	

Promotion process	**Primary**	**Comments**	**Final disposition**
Posts of Responsibility	✓	**Retain indefinitely on master file as it relates to pay/pension etc. (See DES guidelines)**	N/A
Calculation of service	✓	Retain indefinitely on master file	N/A
Promotions/POR Board master files	✓	Retain indefinitely on master file	N/A
Promotions/POR Boards assessment report files	✓	Retain original on personnel file in line with retention periods in "Staff Records" retention guidelines above	N/A
POR appeal documents	✓	Retain original on personnel file, and copy of master & appeal file. Retain for duration of employment + 7 years (6 years in which to take a claim, plus 1 year to serve proceedings on school). Copy on master and appeal file.	N/A
Correspondence from candidates re feedback	✓	Depends upon nature of feedback. If feedback is from unsuccessful candidate who is not an employee within the school, keep in line with retention periods in "Staff Records" above. If feedback is from successful candidate or from unsuccessful candidate who is already an employee within the school, keep in line with "Staff personnel while in employment" above.	N/A

10.4 Government returns:

Government returns	Primary	Comments	Final disposition
Any returns which identify individual staff/pupils,		**Depends upon the nature of the return. If it relates to pay/pension/benefits of staff, keep indefinitely as per DES guidelines. If it relates to information on students, e.g. October Returns, Annual Census etc., keep in line with "Student Records" guidelines above.**	N/A

11. Personal Data Security Breach Code of Practice Form:

Purpose of Code of Practice

This Code of Practice applies to Westport ETNS as data controller.
This Code of Practice will be:

1. available to view in the school office
2. circulated to all staff members

Obligations under Data Protection

The school as data controller is subject to the provisions of the Data Protection Acts, 1988 and 2003 and exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

The school has prepared a **Data Protection Policy** and monitors the implementation of this policy at regular intervals. The school retains records (both electronic and manual) concerning personal data in line with its **Data Protection Policy** and seeks to prioritise the safety of personal data and particularly sensitive personal data, so that any risk of unauthorized disclosure, loss or alteration of personal data is avoided.

Protocol for action in the event of breach

In circumstances where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, Westport ETNS will follow the following protocol**:**

1. The school will seek to contain the matter and mitigate any further exposure of the personal data held. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and requesting that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.

2. Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011. The penalties for withholding information include a fine of up to €5,000 or 12 months' imprisonment on summary conviction.

3. Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the school may conclude that there is no risk to

the data and therefore no need to inform data subjects or contact the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

4. Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (2) above.

5. Contact should be immediately made with the data processor responsible for IT support in the school.

6. In addition and where appropriate, contact may be made with other bodies such as the HSE, financial institutions etc.

7. Reporting of incidents to the Office of Data Protection Commissioner: All incidents in which personal data (and sensitive personal data) has been put at risk shall be reported to the Office of the Data Protection Commissioner as soon as the school becomes aware of the incident (or within 2 working days thereafter), save in the following circumstances:

    - When the full extent and consequences of the incident have been reported without delay directly to the affected data subject(s) **and**
    - The suspected breach affects no more than 100 data subjects **and**
    - It does not include sensitive personal data or personal data of a financial nature[1].

    Where all three criteria are not satisfied, the school shall report the incident to the Office of the Data Protection Commissioner within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident (see further details below). Where no notification is made to the Office of the Data Protection Commissioner, the school shall keep a summary record of the incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record shall comprise a brief description of the nature of the incident and an explanation why the school did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records shall be provided to the Office of the Data Protection Commissioner upon request.

8. The school shall gather a small team of persons together to assess the potential exposure/loss. This team will assist the principal of the school with the practical matters associated with this protocol.

9. The team will, under the direction of the BOM/principal, give immediate consideration to informing those affected [2]. At the direction of the BOM/principal the team shall:

[1/2] Except where law enforcement agencies have requested a delay for investigative purposes. Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows. Where Westport ETNS receives such a direction from law enforcement agencies, they should make careful notes of the advice they receive (including the date and the time of the conversation and the name and rank of the person to whom they spoke). Where possible, Westport ETNS should ask for the directions to be given to them in writing on letter-headed notepaper from the law enforcement agency (eg. An Garda Siochána), or where this is not possible, Westport ETNS should write to the relevant law enforcement agency to the effect that "we note your instructions given to us by your officer [insert officer's name] on XX day of XX at XXpm that we were to delay for a period of XXX/until further notified by you that we are permitted to inform those affected by the data breach."

given to them in writing on letter-headed notepaper from the law enforcement agency (eg. An Garda Siochána), or where this is not possible, Westport ETNS should write to the relevant law enforcement agency to the effect that "we note your

- Contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.
- Where possible and as soon as is feasible, the *data subjects* (i.e. individuals whom the data is about) should be advised of
  - the nature of the data that has been potentially exposed/compromised;
  - the level of sensitivity of this data and
  - an outline of the steps the school intends to take by way of containment or remediation.
- Individuals should be advised as to whether the school intends to contact other organisations and/or the Office of the Data Protection Commissioner.
- Where individuals express a particular concern with respect to the threat to their personal data, this should be advised back to the principal who may, advise the relevant authority e.g. Gardaí, HSE etc.
- Where the data breach has caused the data to be "damaged" (e.g. as a result of hacking), the principal shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.
- The principal shall notify the insurance company which the school is insured and advise them that there has been a personal data security breach.

10. A full review should be undertaken using the template Compliance Checklist *(www.dataprotectionforschools.ie/en/Data-Protection-Guidelines/Compliance-Audit/)* and having regard to information ascertained deriving from the experience of the data protection breach. Staff should be apprised of any changes to the Personal Data Security Breach Code of Practice and of upgraded security measures. Staff should receive refresher training where necessary.

Further advice:

What may happen arising from a report to the Office of Data Protection Commissioner?

- Where any doubt may arise as to the adequacy of technological risk-mitigation measures (including encryption), the school shall report the incident to the Office of the Data Protection Commissioner within **two working days** of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be by e-mail, telephone or fax and shall **not** involve the communication of personal data.
- The Office of the Data Protection Commissioner will advise the school of whether there is a need for the school to compile a detailed report and/or for the Office of the Data Protection Commissioner to carry out a subsequent investigation, based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.
- Should the Office of the Data Protection Commissioner request the school to provide a detailed written report into the incident, the Office of the Data Protection Commissioner will specify a timeframe for the delivery of the report into the incident and the information required. Such a report should reflect careful consideration of the following elements:

  - the amount and nature of the personal data that has been compromised
  - the action being taken to secure and/or recover the personal data that has been compromised

instructions given to us by your officer [insert officer's name] on XX day of XX at XXpm that we were to delay for a period of XXX/until further notified by you that we are permitted to inform those affected by the data breach."

- the action being taken to inform those affected by the incident or reasons for the decision not to do so
- the action being taken to limit damage or distress to those affected by the incident
- a chronology of the events leading up to the loss of control of the personal data; and
- the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the school has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

Personal data Rectification/Erasure Request Form

Request to have Personal Data rectified or erased.

Data Protection Act 1988 and Data Protection (Amendment) Act 2003

Important:

Proof of identity (eg. official/State photographic identity document-drivers licence, passport) must accompany this form.

Full Name	
Address	
Contact number *	Email addresses *

* The school may need to contact you to discuss your access request

Please tick the box which applies to you:

Student ☐	Parent/guardian of student ☐	Former Student ☐	Current Staff ☐	Former Staff ☐
Age: Class:	Name of Student:	Insert Year of leaving:		Insert Years From/To:

I, ……..[insert name] wish to have the data detailed below which Westport ETNS holds about me/my child rectified / erased (*delete as appropriate*). I

am making this access request under **Section 6** of the Data Protection Acts.

Details of the information you believe to be inaccurate and rectification required OR reason why you wish to have data erased:

You must attach relevant documents as proof of correct information e.g. where a date of birth is incorrect, please provide us with a copy of the official State Birth Certificate. Please note that your right to request rectification/deletion is not absolute and may be declined by <Name of school/ETB> in certain cases. You have the right to complain this refusal to the Office of the Data Protection Commissioner: see www.dataprotection.ie .

Signed …… Date ……

Checklist: Have you:

1) Completed the Access Request Form in full? ☐
2) Included document/s as proof of correct information? ☐
3) Signed and dated the Request Form? ☐
4) Included a photocopy of official/State photographic identity document* ☐

***Note to school**: The school should satisfy itself as to the identity of the individual, and make a note in the school records that identity has been provided but the school should not retain a copy of the identity document.

Please address and return this form to:

Chairperson of the Board of Management,
Westport Educate Together National School,
C/O Sharkey Hill Community Centre,
Páirc na Coille
Westport
Co. Mayo
F28 CD82

13. Compliance To Do List:

No.	Item
1.	Have we evaluated our current practices and procedures to ensure that they meet the demands of the Acts?
2.	Have we completed a risk assessment data protection audit using the Compliance Checklist? See Auditing through a Compliance Checklist
3.	Have we appointed an individual to oversee responsibility for data protection?
4.	Have we developed an internal data protection policy? See Data Protection Policy Template **Note to ETB schools**: the school's data protection policy shall be promulgated by the ETB and handed down to the school board of management to be ratified and adopted. In this way, all ETB schools in a ETB area will have consistent Data Protection Policies.
5.	Is a copy of the school/ETB Data Protection Policy sent to all parents/students at enrolment, at the beginning of each academic year and/or when the policy is updated as appropriate in the school/ETB?
6.	Have we developed and adopted a Personal Data Security Breach Code of Practice in case things go wrong? See Personal Data Security Breach Code of Practice Template
7.	Where we have third parties processing personal data for us (e.g. CCTV monitoring companies, external HR/payroll companies, cloud computing, off-site archiving etc.), do we have written data processing agreements/service level agreements in place? See Content of Service Agreements Does this data processing agreement/service level agreement incorporate our school/ETB Personal Data Security Breach Code of Practice?
8.	Awareness and Training: Are all staff aware and have they been properly on their data protection responsibilities? Are all members of staff aware of the school's/ETB's Data Protection Policy and the Personal Data Security Breach Code of Practice? Are refresher courses required?
9.	Are we aware of our security obligations and are we keeping our data safe? Do we have adequate security measures in place such as password protection and an adequate level of encryption? (Note encryption is essential on portable devices holding personal data such as laptops).
10.	Are all staff, parents and students aware of the Guidelines for Taking and Using Images of Children in our School/ETB?
11.	Have we developed and adopted a School/ETB Enrolment Data Protection Statement?
12.	Have we developed and adopted a Personal Data Rectification/Erasure Request Form?
13.	If our school/ETB has a website that collects data from visitors to the site, have we developed and adopted a Website Privacy Statement in consultation with our website designer/provider to ensure that they are correctly and fully disclosing all the information which our school/ETB website gathers and uses and asking for consent where we use cookies? See Website Privacy Statement Template
14.	If our school/ETB has or intends to have a CCTV system in place, have we carried out a Privacy Impact Assessment (see the appendix to the CCTV Policy Form) and have we developed and adopted (in consultation with all relevant parties) a CCTV Policy? See CCTV Policy
15.	Do we have a retention policy in place, and are all members of staff aware of and fully trained in relation to the Records Retention Schedule? See Records Retention Schedule

APPENDIX 1 – DEFINITIONS

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

The Data Protection Acts – The Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All school/ETB staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to 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.

Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

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

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.