

Letterfrack NS Data Protection Policy

New GDPR guidelines necessitate the updating of our record keeping policy to a Data Protection Policy.

Introductory Statement

This Data Protection Policy applies to the personal data held by Letterfrack NS and 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, volunteers, visiting professionals and applicants for staff positions within the school) insofar as the measures under the policy relate to them. The Data Protection Acts apply to the keeping and processing of *personal data*, both in manual and electronic form. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which the school will meet its statutory obligations, to explain those obligations to school staff, students and their parents/guardians and to outline how personal data and sensitive personal data will be protected by the school.

Executive Summary

Letterfrack NS 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. The Education Act 1998, The Education Act Welfare Act 2000 and A guide for Data Controllers.

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. This policy explains what sort of data is collected, why it is collected, for how long it will be stored, and with whom it will be shared.

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

Other Legal Obligations

Implementation of this policy should take account of 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(from 1st January 2014 known as TUSLA), 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 or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training 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 a 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 - CPA (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationship to the characteristic spirit of the school:

We help all children to appreciate moral, spiritual, religious, social and cultural values of their own country and other countries. We promote codes of safety, respect, health and human rights. We the teachers and pupils try to aim to respect 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' right to privacy and rights under the Data Protection Acts.

Aims:

- To ensure the school complies with legislative requirements
- To clarify the types of records maintained and the procedures relating to making them available to the relevant bodies
- To put in place a proper recording and reporting framework on the educational progress of pupils
- To establish clear guidelines on making these records available to parents and pupils over 18
- To stipulate the length of time records and reports will be retained
- To outline how data is to be stored in a safe and secure manner
- To ensure data protection terms are clearly explained **(Appendix 1)**

Personal Data

Letterfrack NS is a data controller of personal data of its past, present and future staff, students, parents/guardians and other members of the school community. To ensure that it is in compliance with current legislation, all personal data requested, obtained and stored must be identified and documented for the whole school community. The Principal and BOM will be responsible for all data protection in the school.

If an individual feels that the information held is incorrect they should complete the “**Personal Data Rectification/Erasure Request Form**” set out at **Appendix 2** and submit it to the Principal or the Chairperson of the Board or Principal.**(Appendix 2)**

Letterfrack NS Data Protection Statement outlines information regarding personal data for parents. This statement will be included on the enrolment form. **(Appendix 3)**

Details of arrangements in place to ensure compliance with the ten rules of data protection:

The policy will be implemented so as to ensure that all personal data records held by the school are obtained, processed, used and retained in accordance with the following ten rules of data protection (based on the Data Protection Acts):

1. Obtain and process information fairly

The school will ensure that data subjects (staff, students, parents, board of management members, etc.) are aware, at the time the personal data is being collected, of the following information:

- the name of the school (the “data controller”)
- the purpose of collecting the data
- the persons or categories of persons to whom the data may be disclosed
- whether replies to questions asked are obligatory and the consequences of not providing replies to those questions
- the existence of the right of access to their Personal Data
- the right to rectify or delete their data if inaccurate, excessive or processed unfairly
- any other information which is necessary so that processing may be fair and to ensure the data subject has all the information that is necessary so as to be aware as to how their data will be processed.

Parents will be required to sign a consent form to allow *Sensitive Personal Data* be collected, store on the POD system and shared with the DES.

In the case of *Sensitive Personal Data*, explicitly given consent is required unless consent may be implied to be given, for example where it is necessary:

- urgently to prevent injury or other damage to the health of a person or to prevent serious loss or damage to property
- for the purpose of obtaining legal advice or in the course of legal proceedings in which the person doing the processing is a party or witness required by or under any enactment or by a rule of law or court order.

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

Letterfrack NS will ensure that the data collected will be done so for the intended purpose and done so in a lawful manner.

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

Under Section 20 of the [Education \(Welfare\) Act, 2000](#), each school principal must maintain a register with the names of all children attending that school. When a child is transferring from

the School, the principal must notify the principal of the new school of any problems relating to school attendance of the child and any other matters relating to the child's educational progress that he or she considers appropriate.

- Incoming student transfer information – 'The Education Passport'

Minister Quinn in June 2012 announced: 'I believe that the sharing of information between primary and second-level schools is a common-sense approach that will benefit both students and teachers. This "education passport" will mean that the child's end-of-year report card, including results from the standardised tests taken in sixth class, will be available to the second level school'.

It is important that assessment information is transferred between schools when students transfer from primary to post-primary school. Each post-primary principal is responsible for informing the principal of each primary school of the names of students for whom enrolment in his or her post-primary school has been confirmed.

Upon receipt of this information, the principal of each primary school is required to send, by the end of the first week of September at the latest, a copy of the end-of-year report card (including the information from standardised tests at sixth class in primary school) to the post-primary school to which a student is transferring. Reporting templates have been developed for this purpose by the NCCA.

- Under Section 28 of the Act, schools may supply *Personal Data*, or information extracted from such data, to other schools or another prescribed body if they are satisfied that it will be used in recording the student's educational history, monitoring the student's educational progress or developing the student's full educational potential. The bodies which have been prescribed (and so can share information) under Section 28 are:
 - The Minister for Education and Skills (which includes the Inspectorate and the National Educational Psychological Service (NEPS))
 - The National Council for Special Education (NCSE)
 - The National Educational Welfare Board (NEWB) (now known as TUSLA)
 - Each school recognised in accordance with section 10 of the Education Act, 1998

Each place designated by the Minister under section 10 of the Education Act, 1998 to be a centre for education.

4. Keep it safe and secure

Letterfrack NS will ensure that data collected will be stored in a safe manner and will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. It will also ensure that any

Third Party with which it shares data, will do so under the confines of a Service Agreement.

Letterfrack NS has a Personal Data Security Breach Code of Practice in place which forms part of any Third Party Service Agreement. (Appendix 4)

5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. All information will be stored in the office filing system or on an encrypted computer Information will only be provided to staff on a “need to know” policy.
8. All waste paper, printouts will be disposed of carefully.
9. Retain it for no longer than is necessary for the purpose or purposes.

Schools are advised by the Department of Education and Skills that school registers and roll books are required to be kept indefinitely within the school.

- Pay, taxation and related school personnel service records should be retained indefinitely within the school, as advised by DES.

- Where litigation may potentially arise in the future (e.g. in relation to accidents/personal injuries involving school personnel/students or accidents occurring on school property, or in relation to school duties or school activities) or where child-safeguarding issues have arisen in relation to a particular student or a particular member of staff (including volunteers), the relevant records should be retained indefinitely or until the possibility of litigation ceases, which may be very many years after the event first occurred. In such cases, schools will need to obtain specific legal advice.

Note: The statute of limitations is a complicated legal issue and varies from case to case. In general, the limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim but the statute of limitations period may be different in every case. In the case of minors who are not suffering under a mental disability or medical condition that would impair their capacity to give their consent, the limitation period does not begin to run until they reach their 18th birthday or later if the date of knowledge post-dates their 18th birthday. In the case of minors with special educational needs, it can be said that the statute of limitations may never expire, and therefore the school may be exposed to litigation many decades after the student has left the school. In the case of any person who has suffered from abuse, in general, the statute of limitations does not begin to run until the person has ceased to be under the “dominion” of that abuse, and determining this is a complex legal issue. There are cases which have come before the courts many decades after the alleged abuse and where the claimant has been successful notwithstanding the passage

of time and where they have taken their claim long after the “normal” statute of limitations period has expired.

In line with the above, it is suggested that the day-to-day ordinary information on student files (such as class work, examination results, report cards) might, as a general rule, be retained for a period of seven years after the student has completed the Senior Cycle and/or reached the age of 18 whichever is the later (ie, 6 years in which to take a claim, plus 1 year for proceedings to be served on the school). However, some records may need to be retained indefinitely, such as those which relate to more sensitive or controversial matters such as:

- child-safeguarding issues
- reports to the HSE/An Garda Síochána
- accidents/personal injuries involving school personnel/students
- accidents occurring on school property, on School trips or in relation to school activities (sports matches etc)
- allegations of bullying or harassment
- disciplinary records, etc.

These records may include data which give additional information and background in relation to particular incidents, including:

- incident report logs
- correspondence to statutory bodies
- notes of meetings
- correspondence with parents
- classroom notes
- playground notes and
- teacher notes.

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

(See Appendix 5) Data Access Procedures Policy and Data Access Request Form

Note: While these rules apply to all computer-held data and any new manual records created from July 2003, they only apply to existing manual records from October 2007.

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.
- (c) **Location:** In a secure, locked filing cabinet (Office or Learning support room) 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:** manual record (personal file within a *relevant locked filing system*), computer record (database) or both are password protected, firewall software, adequate levels of encryption etc.

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). See the template "Guidance on Taking and Using Images of Children in Schools"
- 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. 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
- 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.

- (c) **Location:** In a secure, locked filing cabinet (Office or Learning support room) 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:** manual record (personal file within a *relevant locked filing system*), computer record (database) or both are password protected, firewall software, adequate levels of encryption etc.

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.
- (c) **Location:** In a secure, locked filing cabinet (Office or Learning support room) 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:** manual record (personal file within a *relevant locked filing system*), computer record (database) or both are password protected, firewall software, adequate levels of encryption etc.

D. 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.

- (a) **Location:** In a secure, locked filing cabinet (Office or Learning support room) 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.
- (b) **Security:** manual record (personal file within a *relevant locked filing system*), computer record (database) or both are password protected, firewall software, adequate levels of encryption etc.

Links to other policies and to 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 Behaviour
- Mobile Phone Code
- Admissions/Enrolment Policy
- CCTV Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE/CSPE etc.
-

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.

Dealing with a data access requests

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 using the Data Access Request Form (Appendix 5) 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 using the Data Access Request Form (Appendix 5).

- 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.

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

Ratification & communication

When the Data Protection Policy has been ratified by the board of management, it becomes the school's agreed Data Protection Policy. It should then be dated and circulated within the school community. The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on students, staff and others in the school community.

Parents/guardians and students should be informed of the Data Protection Policy from the time of enrolment of the student e.g. by including the Data Protection Policy as part of the Enrolment Pack, by either enclosing it or incorporating it as an appendix to the enrolment form.

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 should be issued to the board of management to confirm that the actions/measures set down under the policy are being implemented.

Reviewing and evaluating the policy

The policy should be reviewed and evaluated at certain pre-determined times and as necessary. 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 should be revised as necessary in the light of such review and evaluation and within the framework of school planning.

Signed:

For and behalf of board of management

Date:

Appendix 1: Important terms in Data Protection

The following provides a brief explanation of the key terms which should be understood by management and staff in schools. For access to the full statutory definitions used in the Data Protection Acts, you will find a pre-certified restatement of the Data Protection Acts 1988 and 2003 at [View Data Protection Act 1988](#)

Data protection is the means by which the privacy rights of individuals are safeguarded in relation to the processing of their personal data.

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

A **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 accessible. Examples might include student files stored in alphabetical order in a filing cabinet or personnel files stored in schools or in ETB administrative offices.

Personal data is 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. This can be a very wide definition depending on the circumstances.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's:

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

What is meant by the term Data Subject? A data subject is a living individual to whom the data relates.

Data Controllers are those who, either alone or with others, control the contents and use of personal data. Boards of Management of schools are data controllers. In the case of schools under the remit of ETBs, the ETB is the data controller.

What is data processing? Data processing means performing any operation or set of operations on data, including: (i) obtaining, recording or keeping data; (ii) collecting, organising, storing, altering or adapting the data; (iii) retrieving, consulting or using the data, disclosing the information or data by transmitting, disseminating or otherwise making it available; (iv) aligning, combining, blocking, erasing or destroying the data.

Data Processor - a person who processes personal information on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of their employment. For example, an employee of the school (such as the school secretary) would not be a data processor but if the school outsources data to an outside organisation (such as an external payroll company or an archiving service) that organisation could be considered to be a data processor.

Appendix 2

Personal Data Rectification/Erasure Request Form

Letterfrack NS

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 such as 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 <input type="checkbox"/>	Parent/guardian of student <input type="checkbox"/>	Former Student <input type="checkbox"/>	Current Staff <input type="checkbox"/>	Former Staff <input type="checkbox"/>
Age: Year group/class:	Name of Student:	Insert Year of leaving:		Insert Years From/To:

I,[insert name] wish to have the data detailed below which *Letterfrack NS* holds about me/my child rectified / erased. 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 Letterfrack NS 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 (driver's licence, passport, etc.)*.

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

Please address and return this form to: **The Principal or Chairperson of the Board of Management, Letterfrack NS, Letterfrack Co. Galway.**

Appendix 3: Letterfrack NS Data Protection Statement

Letterfrack NS is a data controller under the Data Protection Acts 1988 and 2003. The personal data supplied on our enrolment form is required for the purposes of:

- Student enrolment
- Student registration
- Allocation of teachers and resources to the school
- determining a student's eligibility for additional learning supports
- School administration
- Child welfare (including medical welfare)

While the information provided will generally be treated as private to Letterfrack NS and will be collected and used in compliance with the Data Protection Acts 1988 and 2003, from time to time it may be necessary for us to transfer your personal data to other bodies (including the Department of Education & Skills, the Department of Social Protection, An Garda Síochána, the Health Service Executive, Tusla (CFA) social workers or medical practitioners, the National Educational Welfare Board, the National Council for Special Education, any Special Education Needs Organiser, the National Educational Psychological Service, or (where the student is transferring) to another school). We rely on parents/guardians and students to provide us with accurate and complete information and to update us in relation to any change in the information provided. Should you wish to update or access your/your child's personal data you should write to the school principal requesting an Access Request Form.

Appendix 4

Personal Data Security Breach Code of Practice Form

Letterfrack NS

Personal Data Security Breach Code of Practice

Date:

Purpose of Code of Practice

This Code of Practice applies to *Letterfrack NS* as *data controller* [1]. This Code of Practice will be:

1. available on the school website
2. circulated to all appropriate *data processors* and incorporated as part of the service-level agreement/data processing agreement between the school and the contracted company and
3. shall be advised to staff at induction and at periodic staff meeting(s) or training organised by the school.

Obligations under Data Protection

The school as data controller and appropriate data processors so contracted are 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/ETB 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 unauthorised 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, the school/ETB 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

[1] Unless otherwise indicated, terms used in this Code – such as “personal data”, “sensitive personal data”, “data controller”, “data processor” – have the same meaning as in the Data Protection Acts, 1988 and 2003.

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[2].

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.

[2] ‘personal data of a financial nature’ means an individual’s last name, or any other information from which an individual’s last name can reasonably be identified, in combination with that individual’s account number, credit or debit card number.

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 (and the school's DP Compliance Officer) with the practical matters associated with this protocol.
9. The team will, under the direction of the principal, give immediate consideration to informing those affected^[3]. At the direction of the principal the team shall:
 - 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. Contracted companies operating as data processors: Where an organisation contracted and operating as a *data processor* on behalf of the school becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the school as a matter of urgent priority. In such circumstances, the principal of the school should be contacted directly. This requirement should be clearly set out in the data processing agreement/contract in the appropriate data protection section in the agreement.
10. A full review should be undertaken using the template [Compliance Checklist](#) 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?

[3] 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 Letterfrack NS 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, Letterfrack NS should ask for the directions to be given to them in writing on letter-headed notepaper from the law enforcement agency (eg. An Garda Síochána), or where this is not possible, Letterfrack NS 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."

- 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
 - 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/ETB 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.

Appendix 5

Data Access Request Form

Letterfrack NS

Date issued to data subject:

Access Request Form: Request for a copy of Personal Data under the Data Protection Act 1988 and Data Protection (Amendment) Act 2003

Important: Proof of Identity must accompany this Access Request Form (eg. official/State photographic identity document such as driver's licence, passport).

A fee of €6.35 must accompany this Access Request Form if it is a Section 4 Data Access Request together with proof of identity (eg. official/State photographic identity document such as driver's licence, passport).

Full Name	
Maiden Name <i>(if name used during your school duration)</i>	
Address	
Contact number *	Email addresses *

* We may need to contact you to discuss your access request

Please tick the box which applies to you:

Student <input type="checkbox"/>	Parent/Guardian of student <input type="checkbox"/>	Former Student <input type="checkbox"/>	Current Staff <input type="checkbox"/>	Former Staff <input type="checkbox"/>
Age: Year group/class:	Name of Student:	Insert Year of leaving:		Insert Years From/To:

Section 3 Data Access Request:

I,[insert name] wish to be informed whether or not *Letterfrack NS* holds personal data about me/my child and to be provided with a description of this data and to be informed of the purpose for holding such data. I am making this access request under **Section 3** of the Data Protection Acts.

OR

Section 4 Data Access Request:

I, [insert name] wish to make an access request for a copy of any personal data that *Letterfrack NS* holds about me/my child. I am making this access request under **Section 4** of the Data Protection Acts.

Section 4 Data Access Request only: I attach €6.35

Any other information relevant to your access request (e.g. if requesting images/recordings made by CCTV, please state the date, time and location of the images/recordings (otherwise it may be very difficult or impossible for the school/ETB to locate the data).

Signed Date

Checklist: Have you:

- 5) Completed the Access Request Form in full?
- 6) Included a cheque or postal order made payable to <name of school> in the amount of €6.35 where a Section 4 request is made? (Please do not send us €6.35 if you are making a request under section 3. There is no administration charge for a section 3 request, and if you send us a cheque, it will be returned to you).
- 7) Signed and dated the Access Request Form?
- 8) Included a photocopy of official/State photographic identity document (driver’s licence, passport etc.)*.

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

Please return this form to the relevant address:

Primary Sector: To the Chairperson of Board of Management *Letterfrack NS, Letterfrack, Co. Galway*