BORD OIDEACHAIS AGUS OILIÚNA CHIARRAÍ
KERRY EDUCATION AND TRAINING BOARD

Kerry ETB

Data Protection Policy

Adopted by Kerry ETB on 27th April 2015

Date of next scheduled review of this policy: April 2016

Data Protection Policy

Table of Contents

Appendices

Appendix 1: Data Protection Statement (for inclusion on relevant forms when personal information is being requested)

Appendix 2: Protecting the confidentiality of Personal Data Guidance Note" (CMOD Department of Finance, Dec. 2008)

Appendix 3: Records Management Procedures

Appendix 4: Record Retention Schedule

Appendix 5: Personal Data Rectification/Erasure Form

Appendix 6: Data Access Procedures

Appendix 7: Data Access Request Form

1. Title

Kerry Education and Training Board Data Protection Policy

2. Introductory Statement

2.1. All personal information which Kerry ETB holds is protected by the Data Protection Acts 1988 and 2003. The ETB takes its responsibilities under these laws seriously.

2.2. This policy document will set out, in writing, the manner in which Personal Data relating to staff, students and other individuals (e.g. parents, ETB members, members of board of management etc.) are kept and how the data are protected.

2.3. The functions of the ETB extend to schools, centres and programmes established or maintained by that ETB as well as the ETB's Administrative Centres. Unless otherwise stated in this Policy:

2.3.1. The provisions herein shall apply to all those bodies which are under the remit of the ETB, and

2.3.2. all references within this Policy to "ETB" shall refer to all bodies established or maintained by that ETB.

3. Data Protection Principles

Kerry ETB is a *data controller* of *Personal Data* relating to its past, present and future employees, students, parents, ETB members, members of ETB schools and centres boards of management and various other individuals. As such, the ETB 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:

3.1. **Obtain and process *Personal Data* fairly**: Information on ETB students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous school(s). In relation to information the ETB holds on other individuals (members of staff, individuals applying for positions within the ETB, parents/guardians of students etc.), the information is generally furnished by the individual themselves with full and informed consent, and compiled during the course of their employment or contact with the ETB. 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. This will be achieved by adopting appropriate data protection notices at the point of data capture e.g. Staff Application forms, Student Enrolment Forms. An example of such a notice is set out in **Appendix 1** which contains the **Data Protection Statement** used by Kerry ETB in its student enrolment forms. While an express signature of indication of consent is not necessarily always required, it is strongly recommended, and will be requested, where possible. The minimum age at which consent can be legitimately obtained for processing and disclosure of *Personal Data* is not defined in the Data Protection Acts. However, the Data Protection Commissioner recommends, that, "*as a general rule in the area of education, a student aged eighteen or older may give consent themselves. A student aged from twelve up to and including seventeen should give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. In the case of students under the age of twelve consent of a parent or guardian will suffice.*"

3.2. **Keep it only for one or more specified and explicit lawful purposes**: The ETB 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.

3.3. **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. From time to time it may be necessary for the ETB to disclose employee's personal information to third parties, including: the Department of Education & Skills, Revenue Commissioners, Department of Social Protection, the Central Statistics Office, the Teaching Council, An Garda Síochána, other educational institutions, banks and other financial institutions, past and future employers, auditors, pension administrators, trade unions, staff associations, the Education Training Board Ireland and/or other bodies. Student (and/or parent/guardian) data may be disclosed to third parties including: The Department of Education and Skills (which includes the Inspectorate, and the National Educational Psychological Service (NEPS)), HSE, TUSLA (particularly in relation to Child Protection issues), An Garda Síochana, Universities/Colleges/Institutes, banks (re the awarding of grants/ scholarships) and the Education Training Board Ireland (for the school to obtain advices and support). It may also be necessary to disclose information in order to comply with any legal obligations. Kerry ETB takes all reasonable steps as required by law to ensure the safety, privacy and integrity of the information and, where appropriate, enter into contracts with such third parties to protect the privacy and integrity of any information supplied. Kerry ETB will endeavour to comply with **Department of Finance Guidelines** (copy available at **Appendix 2**) in relation to the transfer of data to third parties.

3.4. **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 ETB 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. Kerry ETB stores personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres, Head Office, schools and centres. The ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The ETB acknowledges that high standards of security are essential for processing all personal information and endeavours to comply with the **Department of Finance Guidelines** (see **Appendix 2**) which contains comprehensive guidelines regarding best practice in the area of data security. Some of the security measures we take include:

- Access to files containing personal data (computerised and manual) is restricted to the staff who work in that particular area e.g. only HR staff have access to personnel files.
- Computer systems are password protected and are backed up daily to a secure server.

- The Administration Centres are secured and alarmed when not occupied.
- Waste paper which may include personal information is confidentially shredded.

All ETB Staff shall adhere to the "Records Management Procedures" of Kerry ETB a copy of which is set out at **Appendix 3**.

3.5. **Keep Personal data accurate, complete and up-to-date:** Students, parents/guardians, and/or staff should inform the ETB of any change which should be made 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 ETB will make all necessary changes to the relevant records. A copy of the Kerry ETB **"Personal Data Rectification/Erasure Form"** is available at **Appendix 5**. The authority to update/amend such records may be delegated to a member of ETB 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. Kerry ETB has procedures in place that are adequate to ensure high levels of data accuracy and completeness and to ensure that personal data is kept up to date. These procedures include:

- Cross-checking of data entry e.g. entering pay details onto payroll system requires one person to enter the data while another person checks for accuracy.
- Files (electronic and manual) are audited periodically by the internal auditors, Internal Audit Unit – ETBs (IAU_ETB) and the Comptroller & Auditor General (C& AG).
- We rely on the individuals who supply personal information (staff, students and others) to ensure that the information provided is correct and to update us in relation to any changes to the information provided. Notwithstanding this, under Section 6 of the Data Protection Acts, individuals have the right to have personal information corrected if necessary.
- If an individual feels that the information held is incorrect they should complete the **"Personal Data Rectification/Erasure Request Form"** set out at **Appendix 5** and submit it to Kerry ETB.

3.6. **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. Personal data held by Kerry ETB will be adequate, relevant and not excessive in relation to the purpose/s for which it is kept. Periodic checks will be made of files (electronic and manual) to ensure that personal data held is not excessive and remains adequate and relevant for the purpose for which it is kept. See **Appendix 3 "Records Management Procedures"** of Kerry ETB and **Appendix 4 "Records Retention Schedule"**.

3.7. **Retain it no longer than is necessary for the specified purpose or purposes for which it was given**: Kerry ETB will have a defined policy on retention periods for personal data and appropriate procedures in place to implement such a policy. For more information on this, see the ETB's **"Record Retention Schedule"** as set out at **Appendix 4** to this Data Protection Policy. As a general rule, where the data relates to an ETB student, the information will be kept for the duration of the individual's time as an ETB student and thereafter may be retained for a further period for a specific purpose depending on the nature or classification of the data. In setting retention periods for different sets of data, regard will be taken of the

relevant legislative and taxation requirements, the possibility of litigation, the requirement to keep an archive for historical purposes and the retention periods laid down by funding agencies e.g. European Structural Funds, NDP. In the case of members of ETB staff, the ETB will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The ETB 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. Retention times cannot be rigidly prescribed to cover every possible situation and the ETB will use the "Record Retention Schedule" as a guideline only. The ETB reserves the right to exercise its judgment and discretion in relation to specific classes of data, taking account of its statutory obligations and best practice in relation to each category of records held.

3.8. **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. On making an access request any individual about whom Kerry ETB keeps *Personal Data*, is entitled to a copy of their personal data and a description of:

- The categories of data being processed,
- The personal data constituting the data of which that person is the subject,
- The purpose for the processing,
- The recipients/categories of recipients to whom the data is or may be disclosed
- Any information known or available to Kerry ETB as to the source of those data unless the communication of that information is contrary to the public interest

To make an access request, the individual should read Kerry ETB's **"Data Access Procedures"** set out at **Appendix 6**, and then complete the **"Data Access Request Form"** set out at **Appendix 7**. Guidance on how Kerry ETB shall handle the Data Access Request is set out at **Appendix 6: "Data Access Procedures"**.

4. Scope

4.1. **Scope:** The functions of Kerry ETB extend to schools, centres and programmes established or maintained by Kerry ETB as well as Kerry ETB's Administrative Centres. Unless otherwise specifically specified in this Policy, this Policy shall apply to all those bodies which are under the remit of Kerry ETB.

4.2. **Purpose of the Policy:** The Data Protection Acts apply to the keeping and processing of *Personal Data*, both in manual form and on computer. The purpose of this Policy is to assist Kerry ETB to meet its statutory obligations while explaining those obligations to staff. The Policy shall also inform staff, Kerry ETB members, students and their parents/guardians how their data will be treated.

4.3. **To whom will the Policy apply?** The Policy applies to all staff, Kerry ETB members, parents/guardians, students and others (including prospective or potential students and their parents/guardians, and applicants for staff positions within Kerry ETB) insofar as Kerry ETB handles or processes their *Personal Data* in the course of their dealings with Kerry ETB.

5. Definition of Data Protection Terms

5.1. **Definitions:** In order to properly understand Kerry ETB's obligations, there are some key terms derived from the Data Protection Acts 1988 and 2003 which should be understood by all relevant staff:

5.1.1. ***Data*** means information in a form that can be processed. It includes both *automated data* (eg. 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.

5.1.2. ***Data Controller*** for the purposes of this Policy is Kerry ETB, but where the Policy is adopted by a Kerry ETB School/Centre, it may also refer to the Board of Management of that School.

5.1.3. ***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. Examples might include student files stored in alphabetic order in a filing cabinet or personnel files stored in the HR office.

5.1.4. ***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 (ie Kerry ETB).

5.1.5. ***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.

6. Rationale

6.1. **Why is it necessary to have a Data Protection Policy?** In addition to its legal obligations under the broad remit of educational and other legislation, Kerry ETB 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.

6.2. 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 Kerry ETB's legal responsibilities has increased. Kerry ETB takes its responsibilities under Data Protection law

very seriously, and wishes to put in place safe practices to safeguard individual's personal data.

6.3. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the Chief Executive and Kerry ETB Board to make decisions in respect of the efficient running of Kerry ETB. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the ETB.

7. Other Legal Obligations

Implementation of this Policy should take account of the legal obligations and responsibilities imposed on both the ETB and ETB Schools. Some legislation places an obligation on the ETB to obtain and retain personal data and is therefore directly relevant to data protection. For example:

7.1. Teaching Council Act 2006.

7.2. Social Welfare Acts.

7.3. Minimum Notice & Terms of Employment Act 1973.

7.4. Payment of Wages Act 1979.

7.5. Pensions Acts 1990-2003.

7.6. Comptroller & Auditor General Act 1993.

7.7. Maternity Protection Acts 1994-2004.

7.8. Organisation of Working Time Act 1997.

7.9. Parental Leave Acts 1998-2006.

7.10. Carers Leave Act 2001.

7.11. Adoptive Leave Act 2005.

7.12. Safety, Health & Welfare at Work Act 2005.

7.13. Various taxation legislation.

7.14. Other employment and equality legislation.

7.15. The ETB is also regulated by Circular Letters and Memos issued by the Department of Education and Skills. These regulations require personal data to be collected, retained by the ETB and in some cases data is to be transferred to DES.

7.16. Education and Training Boards Act 2013

- S.10 Functions of ETBs
- S.11 Additional Functions
- S.27 Duty to prepare and submit a strategy statement to the Minister
- S.30 Composition of ETBs
- Elections to ETBs are conducted under the regulations issued by the Minister[1] pursuant to the power granted under S.3 of the Act of which the following is the relevant:

[1] SI 270/2014 – Education and Training Boards Act 2014 (Election of Staff) Regulations 2014

"election" refers to elections of staff representatives; The Minister is obliged to appoint a returning officer;

(1) duty of returning officer: on appointment "shall cause to be prepared a provisional electoral roll containing the names and addressed of each eligible member of staff";

(3) returning officer must make this roll available for inspection "in the manner the retuning officer considers appropriate";

"The electoral roll of eligible members of staff shall contain the name and address of every eligible member of staff who qualifies to be entered on the roll".

7.17. Education Act 1998

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 his or her education.

7.18. Education (Welfare) Act 2000

(a) Under Section 20 of the Education (Welfare) Act, 2000, the School must maintain a register of all students attending the School. In addition, under section 20(5), 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.

(b) 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.

(c) Under Section 28 of the Education (Welfare) Act, 2000, the School may supply Personal Data kept by it to certain prescribed bodies (the Department of Education and Skills, TUSLA, the National Council for Special Education, 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).

7.19. Education for Persons with Special Educational Needs Act 2004

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.

7.20. Freedom of Information Act 1997

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. If an ETB 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.

Health Act 1947

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.

7.21. *Children First*

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 the Child & Family Agency ("TUSLA") (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

7.22. Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012

Under the Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012, all individuals are mandatorily obliged to disclose information on certain offences against children and against vulnerable adults to An Garda Síochána.

7.23. Youth Work Act 2001

Under Section 9.(1) in addition to the functions conferred on it by or under the ETB Act 2013, each ETB shall, insofar as practicable and within the financial resources available to it (a) ensure the provision within its vocational education area of youth work programmes or youth work services, (*b*) ensure co-ordination within its vocational education area of youth work programmes and youth work services with education programmes and other programmes that provide services for young persons, (*c*) ensure that in the provision of youth work programmes or youth work services, or both, (d) monitor and assess the youth work programmes or youth work services, (*e*) consult with and report to, in regard to youth work, such person or persons as the Minister may, from time to time, direct.

8. Identifying *Personal Data*

The *Personal Data* records held by Kerry ETB at the ETB Administration Centre and held by the ETB School and ETB Centres or by ETB Programmes in their administrative offices may include:

8.1. Staff records

8.1.1. **Categories**: 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,
- date of birth, PPS number
- marital and family details

- educational or previous employment background
- Original records of application and appointment including those relating to promotion posts/in-house applications
- interview records, references
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Records of in-service courses attended
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of complaints and/or grievances and/or disciplinary procedures including consultations or competency discussions, action/improvement/evaluation plans and record of progress. **Note:** A record of grievances may be maintained which is distinct from and separate to individual personnel files.
- Records of any reports 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)
- Superannuation and pension documentation
- Salary, payroll details, bank details.
- Medical information, including the medical questionnaire which employees complete prior to taking up employment, records of sickness absence and medical certificates. Kerry ETB will request all employees to have a medical examination and will therefore hold the resulting medical report. The purpose of keeping this sort of information is to administer sick pay and disability entitlement, monitor and manage sickness absence and to comply with our health and safety obligations. Satisfactory health is one of the conditions of admission to the Superannuation Scheme.
- Information regarding Trade Union membership. Kerry ETB holds this information for the purposes of facilitating the deduction-at-source of union subscriptions.
- Information on commission/alleged commission of offence, any proceedings for an offence. Kerry ETB holds this information to meet the requirements of the Department of Education & Skills and to satisfy itself of the employee's suitability for their position. Garda Vetting records will be retained in compliance with DES C/L 0063/2010 and subsequent relevant circular letters.
- Information regarding disability. Kerry ETB holds this information for the purposes of reporting (on an aggregated, anonymised basis) to the Department of Education and Skills on the target for employment of persons with disability under the Disability Act 2005.

8.1.2. **Purposes**: Staff records are processed and kept for the purposes of:

- For the management and administration of Kerry ETB business now and into the future
- To facilitate the payment of staff, and calculate other benefits/entitlements and to assist the member of staff applying for other benefits/entitlements (including

but not limited to State Illness Benefit, State Disability Allowance, State Invalidity Pension, State Maternity Benefit etc.) to determine reckonable service for the purpose of calculation of pension payments, *ex gratia* or statutory entitlements, and/or redundancy payments where relevant)

- To calculate annual leave allowances or other leave allowances (eg. parental leave, maternity leave etc)
- to facilitate pension payments in the future,
- human resources management,
- to obtain advices on and to address IR/HR matters, disciplinary matters, complaints under the Dignity in the Workplace Policy, complaints made under the grievance policy, and performance management issues. Note: this may involve records being transferred to third parties including the national representative body for Education and Training Boards, ETBI, and legal advisors.
- recording promotions (documentation relating to promotions applied for) and changes in responsibilities
- To enable Kerry ETB 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 Kerry ETB and ETB schools/centres/programmes 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
- For compliance with legislation relevant to the ETB including the generation of electoral registers for the election of staff representatives onto the ETB under the Education and Training Boards Act 2013.

8.1.3. **Location**: Staff records are kept in the Human Resources and Finance departments of the ETB Administration Centres, Head Office. Some records will also be held by the ETB School/ETB Centre. Manual Records will be held 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.

8.1.4. **Security**: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres, Head Office, schools and centres. Where records are held by the ETB School, these will be held in the administrative offices of that School. Manual records are stored in locked filing cabinets, in offices which are accessed only by ETB staff. Automated data is stored on ETB computers and the ETB server. The ETB IT system is password protected, with sufficient firewall software, and adequate levels of encryption The ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The ETB acknowledges that high standards of security are essential for processing all personal information.

8.2. **Student records**

8.2.1. **Categories**: In general student records are kept by the individual ETB schools, ETB centres and programmes run under the auspices of the ETB. These records may include:

(a) Information may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time at the School/Centre/Programme. Information which may be sought and recorded **at enrolment**, including:

- 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

(b) Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student

(c) Psychological, psychiatric and/or medical assessments

(d) Attendance Records

(e) Photographs and recorded images of students (including at school events and noting achievements).

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

(g) Records of significant achievements

(h) Whether the student is repeating the Leaving Certificate

(i) Whether the student is exempt from studying Irish

(j) Records of disciplinary issues and/or sanctions imposed

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

(l) 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)

(m) 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).

8.2.2. **Purposes:** The purposes for obtaining, processing, holding and keeping student records are:

a) To enable each student to develop their full potential.

b) To comply with legislative or administrative requirements.

c) To ensure that eligible students can benefit from the relevant additional teaching or financial supports.

d) To support the provision of religious education.

e) To enable parent/guardians to be contacted in the case of emergency etc. or to inform parents of their child's educational progress or to inform parents of school events etc.

f) To meet the educational, social, physical and emotional requirements of the student.

g) To obtain advice necessary to assist and support the student, and to enable the student to access additional resources etc. Note: this may involve student records being transferred to third parties including: TUSLA, social workers or medical practitioners, the National Council for Special Education, any Special Education Needs Organiser, the National Educational Psychological Service, the national representative body for Education and Training Boards (ETBI), and legal advisors.

h) 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/centre/programme.

i) To ensure that the student meets the ETB admissions criteria.

j) To ensure that students meet the minimum age requirements for their course.

k) To ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities.

l) 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;

m) To furnish, when requested by the student (or their parent/guardian in the case of a student under 18 years) documentation/information/references to third-level educational institutions and/or prospective employers

n) In respect of a work experience placement (where that work experience role requires that the student be Garda vetted) the ETB 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.

o) For compliance with legislation relevant to the ETB including the generation of electoral registers for the election of parent/guardian representatives onto the ETB under the Education and Training Boards Act 2013.

8.2.3. **Location**: Student records will be retained in the ETB Administration Centres, Head Office, schools and centres. The ETB Human Resources Department receives and retains a copy of some student data and documentation, in particular records of student with Special Educational Needs (Psychological Reports which may include name, address and date of birth, PPS Number, psychological assessment (if supplied by school), category of assessed disability parent/guardian name and contact details), and records of non-national students (name, date of birth, nationality and year of entry to Ireland). Note: Some records will also be held by the ETB School. Note: some records may be transferred to third parties as disclosed at (3.3) above. Manual Records will be held 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.

8.2.4. **Security:** Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres, Head Office, schools and centres. Where records are held by the ETB School, these will be held in the administrative offices of that School. Manual records are stored in locked filing cabinets, in offices which are accessed only by ETB staff. Automated data is stored on ETB computers and the ETB server. The ETB IT system is password protected, with sufficient firewall software, and adequate levels of encryption. The ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The ETB acknowledges that high standards of security are essential for processing all personal information.

8.3 Annual Post-Primary School October Return/Examination Entries (known as the "October Returns")

Each year, each recognised post-primary school makes a return to the Department of Education and Skills, the data from which allows the Department of Education and Skills calculate the teaching posts and core funding to be allocated to each recognised post primary school, for the following school year. These returns are made in accordance with *The Rules and Programme for Secondary Schools* via a process called the *Annual Post-Primary School October Return/Examination Entries,* or more commonly known as the 'October Returns'.

8.3.1 Categories: In making their respective returns to the Department, post-primary schools transfer personal data and personal sensitive data on each of their enrolled students (including students who have transferred and are enrolled in the school). Sensitive Data which may be sought at the time of enrolment includes membership of the travelling community and medical card information. This information is sought and retained for the purpose of completion of the 'October Returns'. The 'October Returns' include sensitive personal data regarding personal circumstances which are provided by parents/guardians and students on the basis of explicit and informed consent. The 'October Return' contains individualised data (such as an individual student's PPS number) which acts as an "identifier" for the DES to validate the data that belongs to a recognised student. The DES also transfers some of this data to other Government departments and other State bodies to comply with legislation, such as transfers to the Department of Social Protection pursuant to the Social Welfare Acts, transfers to the State Examinations Commission, transfers to the Educational Research Centre, and transfers to the Central Statistics Office pursuant to the Statistics Acts. The data will also be used by the DES for statistical, policy-making and research purposes. However the DES advises that it does not use individual data, but rather aggregated data is grouped together for these purposes. The DES has a data protection policy which can be viewed on its website (www.education.ie). The DES has also published a "Fair Processing Notice" to explain how the personal data of students and contained in October Returns is processed. This can also be found on www.education.ie (search for Circular Letter 0047/2010 in the "Circulars" section). Explicit permission will be sought from parents/guardians before processing this data in line with DES C/L 47/2010.

8.3.2 Purposes: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres. The ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The ETB acknowledges that high standards of security are essential for processing all personal information.

8.3.3 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.

8.3.4 Security: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres, Head Office, schools and centres. Where records are held by the ETB School, these will be held in the administrative offices of that School. Manual records are stored in locked filing cabinets, in offices which are accessed only by ETB staff. Automated data is stored on ETB computers and the ETB server. The ETB IT system is password protected, with sufficient firewall software, and adequate levels of encryption. The ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The ETB acknowledges that high standards of security are essential for processing all personal information.

8.4 Annual Census for Primary Schools

8.4.1 Categories: Sensitive personal data may be sought at the time of enrolment to Primary School, and sensitive data may also be sought at certain points during the student's time in the school. Sensitive personal data collected for the school to prepare its Annual Census to the Department of Education and Skills includes whether the student is a member of the Traveller Community, and data on religious, ethnic or cultural background. Non-sensitive personal data will also be sought, such as the name, address, gender, PPS number, "mother tongue" of the student and their "year of arrival in Ireland". Some personal data will be gathered relating to the student's parents, eg. mother's maiden name. This information is sought and retained by the Department of Education and Skills for the purpose of *inter alia,* the allocation of resources and/or the completion of the Annual Census. Recognised primary schools must return an Annual Census to the Department of Education and Skills. Where such information is collected for completing these returns, this information should not be used for any other purpose and should be deleted when no longer required. Data on primary school students enrolled as at 30th September is returned to the Department of Education and Skills on an annual basis via the Annual Census. Data on students in the census is only returned in an aggregated format. The DES has a data protection policy which can be viewed on its website (www.education.ie). The DES has also published a "Fair Processing Notice" to explain how the personal data of students and contained in the Annual Census is processed. This can also be found on www.education.ie (search for Circular 17/2014). Explicit permission will be sought from parents/guardians before processing this data in line with DES C/L 17/2014.

8.4.2 Purposes: The only purpose some post-primary schools may collect some of these data is to meet the data requirements for its 'Annual Census' to the Department. The purpose for which the DES collects this information is set out in the DES Fair Processing Notice which can also be found on www.education.ie (search for Circular 17/2014).

8.4.3 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.

8.4.4 Security: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres. The ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The ETB acknowledges that high standards of security are essential for processing all personal information.

8.5 Records of students (and parents/guardians) applying for further education grants and scholarships

Kerry ETB Administration Centre keeps some records of students. Note: Student Universal Support Ireland (SUSI) is the single awarding authority for all student grant applications since the 2012/13 academic year. All new students or students changing course apply to SUSI online. Kerry ETB holds personal data on students (and parent/guardians) who applied for further education grants and scholarships prior to 2012/13 academic year.

8.5.1 Categories of data: These may include information which may have been sought and recorded at application, including:

- name, address and contact details, date of birth, PPS number
- gender, marital and family status (i.e. number of children in family)
- nationality
- details of previous and current/future education
- employment details
- bank details
- name, address and contact details, PPS number of parent/guardian
- marital and family status of parent/guardian
- employment details of parent/guardian
- details of income of parent/guardian

8.5.2 Purposes: to assess eligibility for grant/scholarship and for the administration of the scheme.

8.5.3 Location: records of grant applications are kept in the Education Support Service department of the ETB Administration Centres, <insert address>

8.5.4 Security: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres. The ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss

or destruction. The ETB acknowledges that high standards of security are essential for processing all personal information.

8.6 Examination results

8.6.1 Categories: An ETB school/centre will hold data comprising examination results in respect of its students. These include class, mid-term, annual, continuous assessment and mock- examinations results.

8.6.2 Purposes: The main purpose for which these examination 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 subject choices and levels. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the respective ETB, the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

8.6.3 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.

8.6.4 Security: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres. The ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The ETB acknowledges that high standards of security are essential for processing all personal information.

8.7 Records of students (and parents/guardians) applying for courses/ programmes Kerry ETB runs a number of programmes for children. These include:

- Outdoor education centres activities/educational programmes held at Cappanalea Outdoor Education & Training Centre, Killorglin, Co. Kerry and *Killarney National Park Education Centre, Knockreer, Killarney, Co. Kerry.*
- Music lessons; youth theatre and drama programmes held at Kerry ETB schools.
- Other activities/educational programmes held in various Kerry ETB schools.

The applications for these activities/educational programmes may be accepted by the Kerry ETB Administration centres as well as by the programme concerned.

8.7.1 Categories: These may include: Information which may be sought and recorded at application, including:

- name, address, date of birth, of student,
- details of relevant medical conditions affecting student,
- name, address and contact details of parent/guardian

8.7.2 Purposes: for the administration of the Outdoor Education & Training Centre activities/educational programmes/ Music lessons/Youth Theatre and Drama programme etc.

8.7.3 Location: records of applicants are kept in the Education Support Service department of Kerry ETB Administration Centre, Head Office and/or kept in the administrative offices from which the programme is run. The original application forms are transferred to the centre/programme co-ordinator.

8.7.4 Security: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres. The ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. The ETB acknowledges that high standards of security are essential for processing all personal information.

8.8 Records of students (and parents/guardians of 'under 18s') applying for adult, community and further education courses/programmes

Kerry ETB runs a number of adult and community education programmes. Applications for these courses/programmes may be accepted by Kerry ETB Administration Centres [as well as by the Centre/Programme concerned].

8.8.1 Categories: Information which may be sought and recorded at application, including: name, address and date of birth, PPS Number, Garda Vetting (as required).

8.8.2 Purposes: for the administration of the courses/programmes. Garda Vetting is required for students who, in the course of their work experience, will be in contact with children and/or vulnerable adults.

8.8.3 Location: records of adult, community and further education students are kept in Kerry ETB Administration Centres. [The original application forms are transferred to the Programme Co-ordinator running the programme].

8.8.4 Security: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in Kerry ETB Administration Centres. Kerry ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Kerry ETB acknowledges that high standards of security are essential for processing all personal information.

8.9 ETB, Boards of Management and Selection Boards records

8.9.1 Categories: These may include:

- Name, address and contact details of each member of the ETB, Board of Management and Selection Board (including former members).
- Records in relation to appointments to the ETB/Board.
- Minutes of meetings and correspondence which may include references to particular individuals.
- Travel expenses paid, PPS Number, tax details, bank details.

8.9.2 Purposes: To enable the ETB and Boards of Management to operate in accordance with the Education and Training Boards Act 2013, the Education Act 1998 and other

applicable legislation and to maintain a record of appointments and decisions. To facilitate the payment of members expenses and selection board expenses.

8.9.3 Location: These records are kept in the Finance department and the office of the Chief Executive at Kerry ETB Administration Centres and Head Office.

8.9.4 Security: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in Kerry ETB Administration Centres. Kerry ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Kerry ETB acknowledges that high standards of security are essential for processing all personal information.

8.10 Creditors

8.10.1 Categories of Data: Kerry ETB holds 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.

8.10.2 Purposes: This information is required for routine management and administration of Kerry ETB's financial affairs including the payment of invoices.

8.10.3 Location: These records are kept in the Finance department of Kerry ETB Head Office and ETB schools and centres.

8.10.4 Security: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in Kerry ETB Administration Centres. Kerry ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Kerry ETB acknowledges that high standards of security are essential for processing all personal information.

8.11 Charity Tax-Back Forms

8.11.1 Categories of data: A Kerry ETB school/centre may hold the following data in relation to donors who have made charitable donations to an Kerry ETB school/centre/programme:

- Name
- Address
- Telephone number
- PPS number
- Tax rate
- Signature and
- The gross amount of the donation.

8.11.2 Purposes: Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The information requested on the appropriate certificate is the parent's name, address, PPS number, tax rate, telephone number,

signature and the gross amount of the donation. This is retained by the school in the case of audit by the Revenue Commissioners.

8.11.3 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.

8.11.4 Security: Where applicable, Identify the format in which these records are kept e.g. manual record (personal file within a *relevant filing system*), computer record (database) or both.

8.12 Register of Electors

8.12.1 Categories of Data: Kerry ETB holds some or all of the following information about electors:

- Name,
- address
- Completed ballot paper

8.12.2 Purposes: Under the Education and Training Boards Act 2013, 2 members of Kerry ETB are elected by members of staff of Kerry ETB. Elections are to be held every 5 years and the Administration Centre Staff will prepare a Provisional Electoral Roll from a list of staff. This information is required for the preparation of the provisional and final electoral rolls, the distribution of ballot papers and to maintain a record of the election of staff representatives to the ETB.

8.12.3 Location: These records are kept in the locked room of Kerry ETB Administration Centre, Head Office.

8.12.4 Security: Kerry ETB stores all personal information in controlled access, centralised databases (including computerised and manual files) in the ETB Administration Centres. Kerry ETB will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Kerry ETB acknowledges that high standards of security are essential for processing all personal information.

8.13 CCTV Images/Recordings

8.13.1 Categories: CCTV is installed in some of the ETB's schools, centres and offices, 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 in accordance with Kerry ETB CCTV Policy.

8.13.2 Purposes: Safety and security of staff, students and visitors and to safeguard Kerry ETB property and equipment.

8.13.3 Location: Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is located in the Principal/Manager's office, secure room or in the reception office of each school or centre which can be accessed only by the Principal/Manager.

8.13.4 Security: Kerry ETB recommends the following policy for Kerry ETB schools/centres/office where CCTV is used. 'Access to images/recordings is restricted to the [Chief Executive, Principal Officer, Education Officer/Adult Education Officer, Principal and Deputy Principal of each school and Manager of each centre]. Tapes, DVDs, hard disk 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. [the ETB should identify the format in which these recordings are kept e.g. DVD). Describe applicable security measures, e.g. monitors and recording devices located in locked room etc.]'

9. Links to Other Policies and to Service Delivery

9.1. Our policies need to be consistent with one another, within the framework of the entire ETB. Relevant school policies already in place or being developed or reviewed shall be examined with reference to this Data Protection Policy and any implications which it has for them shall be addressed. This policy should be read in conjunction with the following policy documents applicable to bodies within Kerry ETB (Schools, Centres, Programmes etc):

- Data Breach Management Policy and Procedure Data in ETBs
- Department of Finance Guidance on Protecting the Confidentiality of Personal Data
- Customer Service Charter
- Records Retention Schedule
- CCTV Policy
- Acceptable Usage (ICT) Policy
- Child Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Mobile Phone Code/Policy
- Admissions/Enrolment Policy
- Substance Use Policy
- Employee Handbook [/Disciplinary Policy] etc.

Note: Where relevant and applicable to students, a number of these policies may be made available by the ETB school/centre/administration centre concerned on/following student enrolment.

10. Dealing with Data Access Requests

10.1. **Section 3 Access Request:** Under section 3 of the Data Protection Acts, an individual has the right to be informed whether the data controller holds data 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.

10.2. 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.

10.3. **Section 4 Access Request:** Individuals are entitled to a copy of their personal data on written request:

10.3.1. 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).

10.3.2. Request must be responded to within 40 days.

10.3.3. Fee may apply but cannot exceed €6.35

10.3.4. Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the ETB 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.

10.3.5. 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 ETB refuse to furnish the data to the applicant.

11. Providing information over the 'phone'

11.1. In Kerry ETB Head Office/schools/centres, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the Head Office/school/centre over the phone. In particular the employee concerned should:

- Check and verify the identity of the caller to ensure that information is only given to a person who is entitled to that information.
- Request 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 Manager/Principal/ETB Co-ordinator for assistance in difficult situations.
- No employee should feel forced into disclosing personal information.

12. Implementation Arrangements, Roles and Responsibilities

12.1. The Chief Executive of Kerry ETB and delegated Officers i.e. the Principal Officer, School Principals, Centre Managers and Section Heads are responsible for implementing this Policy, and for ensuring that staff who handle or have access to Personal Data are familiar with their data protection responsibilities. However all employees who collect and/or control the contents and use of personal data are individually responsible for compliance with the data protection legislation. Kerry ETB will provide support, advice and training to all staff concerned to ensure compliance with the legislation.

12.2. Within Kerry ETB, the following personnel will have responsibility for implementing the Data Protection Policy:

Name/Role	Responsibility
ETB	Data Controller
Chief Executive, Principal Officer, ETB School Principals, Centre Managers, Section Heads, ETB School Board of Management	Implementation of Policy
Teaching personnel	Awareness of responsibilities
Administrative personnel	Security, confidentiality
IT personnel	Security, encryption, confidentiality

13. Ratification & Communication

13.1 This Policy was adopted by Kerry ETB at its ETB meeting on 27th April, 2015 and came into operation immediately.

13.2 This Policy was ratified and adopted by [insert name of ETB School/Centre/Programme] on [insert date].

13.3 It will shortly be published on the Kerry ETB website www.kerryetb.ie where it can be accessed by all staff, students and their parents and members of the public.

13.4 The policy will be brought to the attention of all Kerry ETB staff. All Kerry ETB staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements.

13.5 The Data Protection Policy shall be brought to the attention of new members of ETB staff during their induction training.

13.6 Kerry ETB students and their parents/guardians shall be informed of the Data Protection Policy from the time of enrolment of the student, eg. 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.

14. Monitoring the implementation of the Policy

14.1 The implementation of the Policy will be monitored by the Chief Executive and delegated officers of Kerry ETB.

14.2 At least one annual report shall be issued to the ETB board to confirm that the actions/measures set down under this Data Protection Policy are being implemented.

15. Reviewing and evaluating the Policy

15.1. The Policy will be reviewed and evaluated at certain predetermined times and as necessary.

15.2. Ongoing review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills, Internal Audit Unit-ETBs (IAU-ETB), C&AG or TUSLA), legislation and feedback from parents/guardians, students, staff and others.

15.3. This Policy shall be revised as necessary in the light of such reviews and evaluations and within the framework of ETB planning.

BORD OIDEACHAIS AGUS OILIÚNA CHIARRAÍ
KERRY EDUCATION AND TRAINING BOARD

Kerry ETB

Data Protection Policy

Appendices

Adopted by Kerry ETB on 27th April 2015

Date of next scheduled review of this policy: April 2016

Appendices

Appendix 1: Data Protection Statement (for inclusion on relevant forms when personal information is being requested)

Appendix 2: Protecting the confidentiality of Personal Data Guidance Note" (CMOD Department of Finance, Dec. 2008)

Appendix 3: Records Management Procedures

Appendix 4: Record Retention Schedule

Appendix 5: Personal Data Rectification/Erasure Form

Appendix 6: Data Access Procedures

Appendix 7: Data Access Request Form

Appendix 1

Data Protection Statement

(for inclusion on relevant forms when personal information is being requested)

Personal Data on this Form:

Kerry ETB is a data controller under the Data Protection Acts 1988 and 2003. The personal data supplied on this _____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 and transportation,
- examinations
- school administration,
- child welfare (including medical welfare)
- and to fulfil our other legal obligations.

ETB Contacting You

Please confirm if you are happy for us to contact you by SMS/text message, and to call you on the telephone numbers provided and to send you emails for all the purposes of:

- sports days,
- parent teacher meetings,
- school concerts/events,
- to notify you of school closure (eg. where there are adverse weather conditions),
- to notify you of your child's non-attendance or late attendance or any other issues relating to your child's conduct in school,
- to communicate with you in relation to your child's social, emotional and educational progress, and to contact you in the case of an emergency

Tick box if "yes" you agree with these uses

Use your email address to alert you to these issues? ☐

Use your mobile phone number to send you SMS texts to alert you to these issues? ☐

Use your mobile phone/landline number to call you to alert you to these issues? ☐

Please note: *<Name of ETB>* reserves the right to contact you in the case of an emergency relating to your child, regardless of whether you have given your consent.

School sending you direct marketing

We would like to send you emails/SMS text messages or call you or to write to you at your home address to inform you of special offers or promotions by certain third parties involved in the supply of school stationery and school uniform supplies etc. (eg. [disclose name of organisation/company]). Do you give your consent for us to do each of the following:

Tick box if "yes" you agree with these uses

Use your email address to alert you to these offers?	☐
Use your mobile phone number to send you SMS texts in relation to these offers?	☐
Use your mobile phone/landline number to call you in relation to these offers?	☐
Use your address to send you written letters/brochures in relation to these offers?	☐

While the information provided will generally be treated as private to *<Name of ETB>*, 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 on a private basis to other bodies (including the Department of Education & Skills, the Department of Social Protection, An Garda Síochána, the Health Service Executive, TUSLA, social workers or medical practitioners, the National Council for Special Education, any Special Education Needs Organiser, the National Educational Psychological Service, or (where the student is transferring) with 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.

Data Protection Policy: A copy of the full Data Protection Policy enclosed in this enrolment pack, and you and your child should read it carefully. When you apply for enrolment, you will be asked to sign that you consent to your data/your child's data being collected, processed and used in accordance with this Data Protection Policy during the course of their time as a student in the school. Where the student is over 18 years old, they will be asked to sign their consent to this.

Photographs of Students: The ETB maintains a database of photographs of ETB events held over years. It has become customary to take photos of students engaged in activities and events in the interest of creating a pictorial as well as historical record of life at the school/centre. Photographs may be published on our website or in brochures, yearbooks, newsletters, local and national newspapers and similar school-related productions. In the case of website photographs, student names will not appear on the website as a caption to the picture. If you or your child wish to have his/her photograph removed from the school website, brochure, yearbooks, newsletters etc. at any time, you should write to the ETB Chief Executive.

Consent *(tick one only)*

1. **If you are happy to have your child's photograph taken as part of ETB activities and included in all such records tick here** ☐
2. **If you would prefer not to have your child's photograph taken and included in such records, please tick here** ☐
3. **If you are happy for your child's photograph to be taken and included, as *1.* above, but would prefer not to have images of your child appear on the website, in school brochures, yearbooks, newsletters etc please tick here.** ☐

Signed: _____
Parent/Guardian/Student (where over 18)

Date: _____

Note to ETB School/Centre/Programme: enclose a copy of Kerry ETB Data Protection Policy in the enrolment pack.

Appendix 2

"Protecting the confidentiality of Personal Data Guidance Note" **(CMOD Department of Finance, Dec. 2008)**

Taken from https://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf

Protecting the confidentiality of Personal Data

Guidance Note

CMOD
Department of Finance
December 2008

Contents

Introduction

Under the Data Protection Acts, 1988 and 2003, Government Departments, Offices and Agencies, as data controllers, have a legal responsibility to:-

- obtain and process personal data fairly;
- keep it only for one or more specified and explicit lawful purposes;
- process it only in ways compatible with the purposes for which it was given initially;
- keep personal data safe and secure;
- keep data accurate, complete and up-to-date;
- ensure that it is adequate, relevant and not excessive;
- retain it no longer than is necessary for the specified purpose or purposes; and,
- provide a copy of his/her personal data to any individual, on request.

The purpose of these guidelines is to assist Departments, Offices and Agencies in implementing systems and procedures that will ensure, as much as possible, that personal data in their possession is kept safe and secure and to help Departments, Offices and Agencies meet their legal responsibilities as set out above. This document can be expanded upon by Departments[1] to create detailed policies and procedures which reflect their specific business requirements.

Any queries in relation to the content of this document should be forwarded via email to dpguidelines@finance.gov.ie

Scope

This document provides guidelines on how personal data is to be stored, handled and protected under the following headings:-

a. General Procedures;

[1] For "Departments" read "Departments, Offices and Agencies" throughout this document

b. Paper Records;

c. Email and Personal Productivity Software;

d. Electronic Remote Access;

e. Laptops/Notebooks;

f. Mobile Storage Devices;

g. Data Transfers;

h. Inappropriate Access/Audit Trail Monitoring;

i. Breach Management.

Audience

The information contained in this document is intended for general distribution. However, it is especially important that senior management in Departments are aware of the contents of the document as the responsibility rests with them to ensure that the guidelines contained in it are followed. The guidelines should also be brought to the attention of all staff whose work involves the handling of personal data.

General Procedures

This document sets out guidelines in a number of specific areas where particular attention should be paid in order to help protect the confidentiality of personal data held in a Department. There are, however, a number of general procedures which Departments should follow:-

1. The first stage in establishing policies and procedures to ensure the protection of personal data is to know what data is held, where it is held and what the consequences would be should that data be lost or stolen. With that in mind, as a first step Departments should conduct an audit identifying the types of personal data held within the organisation, identifying and listing all information repositories holding personal data and their location. Risks associated with the storage, handling and protection of this data should be included in the Department's risk register. Departments can then establish whether the security measures in place are appropriate and proportionate to the data being held while also taking on board the guidelines available in this document;

2. Access to all data centres and server rooms used to host hardware and software on which personal data is stored should be restricted only to those staff members that have clearance to work there. This should, where possible, entail swipe card and/or PIN technology to the room(s) in question - such a system should record when, where and by whom the room was accessed. These access records and procedures should be reviewed by management regularly;

3. Access to systems which are no longer in active use and which contain personal data should be removed where such access is no longer necessary or cannot be justified;

4. Passwords used to access PCs, applications, databases, etc. should be of sufficient strength to deter password cracking or guessing attacks. A password should include numbers, symbols, upper and lowercase letters. If possible, password length should be around 12 to 14 characters but at the very minimum

8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. Departments must also ensure that passwords are changed on a regular basis;

5. Departments should have procedures in place to properly evaluate requests from other organisations for access to personal data in its possession. Such procedures should assist Departments in assessing whether the release of personal data is fully justifiable under the Data Protection Acts. Departments should also ensure that access by staff of personal data for analysis or research purposes is fully justifiable and proportionate;

6. Personnel who retire, transfer from the Department, resign etc. should be removed immediately from mailing lists and access control lists. Relevant changes should also occur when staff are transferred to other assignments internally. It is the responsibility of Departments to ensure that procedures are in place to support this, i.e. so that notification is provided to the relevant individual(s)/Unit in a timely fashion;

7. Contractors, consultants and external service providers employed by Departments should be subject to strict procedures with regard to accessing personal data by way of formal contract in line with the provisions of the Data Protection Acts. The terms of the contract and undertakings given should be subject to review and audit to ensure compliance;

8. Departments should have in place an up-to-date Acceptable Usage Policy in relation to the use of Information and Communications Technology (e.g. telephone, mobile phone, fax, email, internet, intranet and remote access, etc.) by its staff. This policy should be understood and signed by each user of such technology in the Department;

9. Departments' Audit Committees, when determining in consultation with Secretaries General (or CEOs, etc. where relevant) the work programme of their Internal Audit Units (IAUs), should ensure that the programme contains

adequate coverage by IAUs of areas within their organisations which are responsible for the storage, handling and protection of personal data. The particular focus of any review by IAUs would be on assessing the adequacy of the control systems designed, in place and operated in these areas for the purpose of minimising the risk of any breach of data protection regulations. Risks associated with the storage, handling and protection of personal data should be included in the Department's risk register and risk assessments should take place as part of a Department's risk strategy exercise. Furthermore, external audits of all aspects of Data Protection within the organisation may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

10. Procedures should be put in place in relation to disposal of files (both paper and electronic) containing personal data. In doing so, Departments should be aware of their legal obligations as set out in the National Archives Act, 1986 and the associated National Archives Regulations, 1988. It should be noted that incoming and outgoing emails which are 'of enduring interest' are archivable records under the Act. Procedures should also be put in place in relation to the secure disposal of computer equipment (especially storage media) at end-of-life. This could include the use of degaussers, erasers and physical destruction devices, etc;

11. Quality Customer Service documentation/customer charters should detail how customers' data is held and how it will be used/not used. Website privacy statements should be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data;

12. New staff should be carefully coached and trained before being allowed to access confidential or personal files;

13. Staff should ensure that callers to the office or other unauthorised persons are unable to view personal or sensitive information whether held on paper documents or information displayed on PC monitors, etc.;

14. All staff should ensure that PCs are logged off or 'locked' when left unattended for any period of time (e.g. in Windows, using Ctrl+Alt+Del keys). Where possible, staff should be restricted from saving files to the local disk. Users should be instructed to only save files to their allocated network drive;

15. Personal and sensitive information should be locked away when not in use or at end of day;

16. Appropriate filing procedures (both paper and electronic) should be drawn up and followed;

17. Departments should be careful in their use of the Personal Public Service Number (PPSN) in systems, on forms and documentation. There is a strict statutory basis providing for the use of the PPSN. This allows organisations use the PPSN in support of a provision of a public service to a customer. The Department of Social & Family Affairs manages the issuance and use of PPS Numbers. A register of organisations that use the PPSN has been prepared and published to promote transparency regarding the ongoing use and future development of the PPSN as a unique identifier for public services. The register is available at: http://www.welfare.ie/EN/Topics/PPSN/Pages/rou.aspx .

18. Any databases or applications in use by Departments which contain personal data must be registered with the Office of the Data Protection Commissioner.

Paper Records

The Data Protection Acts apply equally to personal data held on ICT systems and on paper files. The following guidelines should be followed with regard to personal and sensitive data held on paper files:-

1. Paper records and files containing personal data should be handled in such a way as to restrict access only to those persons with business reasons to access them;

2. This should entail the operation of a policy whereby paper files containing such data are locked away when not required;

3. Consideration should also be given to logging access to paper files containing such data and information items;

4. Personal and sensitive information held on paper must be kept hidden from callers to offices;

5. Secure disposal of confidential waste should be in place and properly used. If third parties are employed to carry out such disposal, they must contractually agree to the Department's data protection procedures and ensure that the confidentiality of all personal data is protected. Such contracts should contain clauses similar to those outlined in the section on 'Data Transfers' below;

6. When paper files are transferred within a Department, this usually entails hand delivery. However, it should be noted that, in many cases, internal post in Departments ultimately feeds into the general postal system (this is particularly true for Departments with disparate locations). In these instances, senders must consider registered mail or guaranteed parcel post service where appropriate. Procedures must be in place for ensuring that the data is delivered only to the person to whom it is addressed, or another officer clearly acting on their behalf,

and not any other staff member. Consideration should also be given to the security of manual files when in transit internally;

7. Facsimile technology (fax machines) should not be used for transmitting documents containing personal data.

Email and Personal Productivity Software

Email and other personal productivity software such as word processing applications, spreadsheets, etc. are valuable business tools which are in use across every Department. However, Departments must take extreme care in using this software where personal and sensitive data is concerned. In particular:-

1. Standard unencrypted email should **never** be used to transmit any data of a personal or sensitive nature. Departments that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted either through file encryption or through the use of a s***ecure email*** facility which will encrypt the data (including any attachments) being sent. The strongest encryption methods available should be used. Departments should also ensure that such email is sent only to the intended recipient. In order to ensure interoperability and to avoid significant key management costs, particular attention should be paid to any central solutions put in place for this purpose;

2. Departments should consider implementing solutions that scan outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission;

3. Where personal or sensitive data is held on applications and databases with relevant security and access controls in place, additional controls should be considered that would prevent such data from being copied to personal productivity software (such as word processing applications, spreadsheets, etc.) where no security or access controls are in place and/or can be bypassed.

Remote Access

There is an increasing business requirement for mobile working and e-working across the public service. Consequently, the demand from staff to access remotely the same systems that they can access from the office is increasing. This brings its own challenges in relation to data security which Departments must address. With regard to personal and sensitive data, the following guidelines should be adhered to:-

1. In the first instance, all personal and sensitive data held electronically should be stored centrally (e.g. in a data centre or in a Department's secure server room with documented security in place). Data that is readily available via remote access should not be copied to client PCs or to portable storage devices, such as laptops, memory sticks, etc. that may be stolen or lost;

2. When accessing this data remotely, it must be done via a secure encrypted link (e.g. IPSEC or SSL VPN tunnel) with relevant access controls in place;

3. Additional stringent security and access controls should be in place, e.g. the mandatory use of strong passwords and security token authentication (i.e. two-factor authentication);

4. Data being accessed in this way should be prevented from being copied from the central location to the remote machine;

5. Departments must utilise technologies that will provide for the automatic deletion of temporary files which may be stored on remote machines by its operating system;

6. Departments should ensure that only known machines (whether desktop PC, laptop, mobile phone, PDA, etc.) configured appropriately to the Department's standards (e.g. with up-to-date anti-virus and anti-spyware software, full encryption, etc.), are allowed to remotely access centrally held personal or sensitive data. The strongest encryption methods available should be used to

encrypt data on these machines. In addition, 'strong' passwords/passphrases (see 'General Procedures') must be used to protect access to these machines and to encrypt/decrypt the data held on them;

7. Staff should be aware that it is imperative that any wireless technologies/networks used when accessing the Department's systems should be encrypted to the strongest standard available.

Laptops and Other Mobile Storage Devices (incl. Mobile Phones, PDAs, USB memory sticks, External Hard Drives, etc.)

The use of laptops, USB memory sticks and other portable or removable storage has increased substantially in the last number of years. Likewise, the use of personal communications and storage devices such as mobile phones, PDAs, etc. has also increased. These devices are useful tools to meet the business needs of staff. They are, however, highly susceptible to loss or theft. To protect the content held on these devices, the following recommendations should be followed:

1. All portable devices should be password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, both a PIN and login password should be used. Manufacturer or operator-provided PIN codes must be changed from the default setting by the user on receipt of the device;

2. Passwords used on these devices should be of sufficient strength to deter password cracking or guessing attacks. A password should include numbers, symbols, upper and lowercase letters. Password length should ideally be around 12 to 14 characters but at the very minimum 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. Departments must ensure that passwords are regularly changed;

3. Personal, private, sensitive or confidential data should not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be encrypted. With regard to laptops, full disk encryption must be employed regardless of the type of data stored;

4. With regard to mobile technologies, staff should be aware that when 'roaming' abroad, communications may not be as secure as they would be within Ireland;

5. Data held on portable devices should be backed up regularly to the Department's servers;

6. When portable computing devices are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons;

7. Portable devices must not contain unauthorised, unlicensed or personally licensed software. All software must be authorised and procured through a Department's IT Unit;

8. Anti-virus/Anti-spyware/Personal Firewall software must be installed and kept up to date on portable devices. These devices should be subjected to regular virus checks using this software;

9. Departments should ensure that when providing portable devices for use by staff members, each device is authorised for use by a specific named individual. The responsibility for the physical safeguarding of the device will then rest with that individual;

10. Laptops must be physically secured if left in the office overnight. When out of the office, the device should be kept secure at all times;

11. Portable devices should never be left in an unattended vehicle;

12. Portable storage media should only be used for data transfer where there is a business requirement to do so, should only be used on approved workstations and must be encrypted;

13. In order to minimise incidents of unauthorised access and/or incidents of lost/stolen data, Departments should restrict the use of personal storage media and devices (e.g. floppy disks, CDs, DVDs, USB memory sticks, etc.) to staff that require to use these media/devices for business purposes;

14. Only storage media provided by a Department's IT Unit should be permitted for use with that Department's computer equipment. Departments must put in place solutions which only allow officially sanctioned media to be used on a Department's computer equipment (i.e. on networks, USB ports, etc.);

15. Staff owned devices such as portable media players (e.g. iPods, etc.), digital cameras, USB sticks, etc. must be technologically restricted from connecting to Department computers;

16. Departments should consider implementing additional log-in controls on portable devices such as laptops;

17. Departments should implement technologies that will allow the remote deletion of personal data from portable devices (such as mobile phones and PDAs) should such devices be lost or stolen. A procedure for early notification of such loss should be put in place. This would allow for the disconnection of the missing device from a Department's email, calendar and file systems;

18. Departments should implement procedures that will ensure that personal data held on mobile storage devices is fully deleted when the data is no longer required (e.g. through fully formatting the devices' hard drive);

Data Transfers

Data Transfers are a daily business requirement for most, if not all, Government Departments. With regard to personal and sensitive data, such transfers should take place only where absolutely necessary, using the most secure channel available. To support this, Departments should adhere to the following:-

1. Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted rather than copying to media for transportation. Where this is not possible or appropriate at present, the safety of the data should be ensured before, during and after transit;

2. Manual data transfers using removable physical media (e.g. memory sticks, CDs, tape, etc.) should end where possible;

3. In the meantime, where data is copied to removable media for transportation such data must be encrypted using the strongest possible encryption method available. Strong passwords/passphrases (see 'General Procedures') must be used to encrypt/decrypt the data;

4. Any such encrypted media should wherever possible be accompanied by a member of the Department's staff, be delivered directly to, and be signed for by, the intended recipient. If this is not possible, the use of registered post or another certifiable delivery method may be used if an agreement similar to that outlined in 7. below has been put in place;

5. 'Strong' passwords (see 'General Procedures') must be used to protect any encrypted data. Such passwords must not be sent with the data it is intended to protect. Care should be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person;

6. Standard email should never be used to transmit any data of a personal or sensitive nature. Departments that wish to use email to transfer such data must

ensure that personal or sensitive information is encrypted either through file encryption or through the use of a ***secure email*** facility which will encrypt the data (including any attachments) being sent. Staff should ensure that such mail is sent only to the intended recipient. In order to ensure interoperability and to avoid significant key management costs, particular attention should be paid to any central solutions put in place for this purpose;

7. When a data transfer with a third party is required (including to/from other Government Departments), a written agreement should be put in place between both parties in advance of any data transfer. Such an agreement should define:-

- The information that is required by the third party (the purposes for which the information can be used should also be defined if the recipient party is carrying out processing on behalf of the organisation);
- Named contacts in each organisation responsible for the data;
- The frequency of the proposed transfers;
- An explanation of the requirement for the information/data transfer;
- The transfer method that will be used (e.g. Secure FTP, Secure email, etc.);
- The encryption method that will be used;
- The acknowledgement procedures on receipt of the data;
- The length of time the information will be retained by the third party;
- Confirmation from the third party that the information will be handled to the same level of controls that the Department apply to that category of information;
- Confirmation as to the point at which the third party will take over responsibility for protecting the data (e.g. on confirmed receipt of the data);
- The method of secure disposal of the transfer media and the timeline for disposal;
- The method for highlighting breaches in the transfer process;
- For data controller to data controller transfers (as opposed to a data controller to a data processor transfer), it needs to be clear that only necessary data is transferred to meet the purposes;

- Business procedures need to be in place to ensure that all such transfers are legal, justifiable and that only necessary data is transferred to meet the purposes;
- Particular attention should be focussed on data made available to third party data processors under contract for testing purposes. Live data should not be used for this purpose.

Appropriate Access and Audit Trail Monitoring

All organisations have an obligation to keep information 'safe and secure' and have appropriate measures in place to prevent "unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction" in compliance with sections 2(1)(d) and 2C of the Data Protection Acts 1988 & 2003. It is imperative, therefore, that Departments have security in place to ensure that only those staff members with a business need to access a particular set of personal or sensitive data are allowed to access that data. In addition to this general requirement, the following guidelines should be followed:-

1. Departments should ensure that their ICT systems are protected by use of appropriate firewall technologies and that this technology is kept up-to-date and is sufficient to meet emerging threats;

2. In order to capture instances of inappropriate access (whether internal or external), addition, deletion and editing of data, audit trails should be used where technically possible. In situations where systems containing personal data do not currently record 'view' or 'read' access, it should be investigated, as a matter of urgency whether such functionality can be enabled. In carrying out such an investigation, Departments should take into account whether there would be any effect on system performance that may hinder the ability of the Department to conduct its business. If the functionality cannot be enabled and the risk of inappropriate access is sufficiently high, such systems should be scheduled for removal from use and replaced by systems with appropriate auditing functionality;

3. Access to files containing personal data should be monitored by supervisors on an ongoing basis. Staff should be made aware that this is being done. IT systems may need to be put in place to support this supervision.

Breach Management

A data security breach can happen for a number of reasons, including:-

- Loss or theft of data or equipment on which data is stored (including break-in to an organisation's premises);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a flood or fire;
- A hacking attack;
- Access where information is obtained by deceiving the organisation that holds it.

It is important that Departments put into place a breach management plan to follow should such an incident occur. There are five elements to any breach management plan:-

1. Identification and Classification
2. Containment and Recovery
3. Risk Assessment
4. Notification of Breach
5. Evaluation and Response

1. Identification and Classification

Departments must put in place procedures that will allow any staff member to report an information security incident. It is important that all staff are aware to whom they should report such an incident. Having such a procedure in place will allow for early recognition of the incident so that it can be dealt with in the most appropriate manner.

Details of the incident should be recorded accurately, including the date and time the incident occurred, the date and time it was detected, who/what reported the incident,

description of the incident, details of any ICT systems involved, corroborating material such as error messages, log files, etc. In this respect, staff need to be made fully aware as to what constitutes a breach.

2 Containment and Recovery

Containment involves limiting the scope and impact of the breach of data protection procedures.

If a breach occurs, Departments should:-

- decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation;
- establish who in the organisation needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. For example, this might entail isolating a compromised section of the network, finding a lost file or piece of equipment, or simply changing access codes to server rooms, etc.;
- establish whether there is anything that can be done to recover losses and limit the damage the breach can cause;
- where appropriate, inform the Garda.

3. Risk Assessment

In assessing the risk arising from a data security breach, Departments should consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be. In assessing the risk, Departments should consider the following points:-

- what type of data is involved?;

- how sensitive is it?;
- are there any protections in place (e.g. encryption)?;
- what could the data tell a third party about the individual?;
- how many individuals' personal data are affected by the breach?;

4. Notification of Breaches

Although there is no current explicit legal obligation to notify individuals or other bodies under the Data Protection Acts of a breach, the Data Protection Commissioner's Office encourages voluntary notification and early engagement with the Office. Therefore, if inappropriate release/loss of personal data occurs it should be reported immediately, both internally and to the Data Protection Commissioner's Office and, if appropriate in the circumstances, to the persons whose data it is. In this regard, Departments should be aware of the dangers of 'over notifying'. Not every incident will warrant notification. For example, notifying a whole 200,000 strong customer base of an issue affecting only 2,000 customers may cause disproportionate enquiries and work.

When notifying individuals, Departments should consider using the most appropriate medium to do so. They should also bear in mind the security of the medium used for notifying individuals of a breach of data protection procedures and the urgency of the situation. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and what the Department is willing to do to assist them. Departments should also provide a way in which individuals can make contact for further information, e.g. a helpline number, webpage, etc.

Departments should consider notifying third parties such as the Garda, bank or credit card companies who can assist in reducing the risk of financial loss to individuals.

The Office of the Data Protection Commissioner will provide advice upon notification as to the requirement or otherwise, in particular circumstances, to notify individuals.

5. Evaluation and Response

Subsequent to any information security breach a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

Any recommended changed to policies and/or procedures should be documented and implemented as soon as possible thereafter.

Each Department should identify a group of people within the organisation who will be responsible for reacting to reported breaches of security.

Appendix 3

Records Management Procedures

Note to ETBs: this is an internal document for internal ETB use only. This Appendix does not have to be circulated to students/parents

1. Purpose

Good records management is of special significance in the context of Kerry ETB's functions, where the maintenance of academic records is a core activity. We aim to implement records management procedures and to ensure preservation of records of permanent value and to establish archival criteria to maintain and assure continued access to appropriate historical records.

2. Ownership of Records

All records, irrespective of format, (i.e. both manual and automated data) created or received by ETB staff in the course of their duties on behalf of Kerry ETB , are the property of Kerry ETB and subject to its overall control. Any employees leaving Kerry ETB or changing positions within Kerry ETB must leave all records intact for their successors and is not permitted to remove or retain records (in electronic or manual format) for any reason.

3. Management of ETB Records

3.1. All records created and received by ETB staff in the course of their duties on behalf of Kerry ETB must be retained for as long as they are required to meet the legal, administrative, financial and operational requirements of Kerry ETB, after which time they are either destroyed or transferred to Kerry ETB archives.

3.2. The final disposition (either destruction or transfer to the archives) of records is carried out according to approved Records Retention Schedules as appended to the Kerry ETB Data Protection Policy.

3.3. While the Records Retention Schedule (set out at Appendix 4 of the Kerry ETB Data Protection Policy) prescribes the minimum period that ETB records must be retained, officers may, at their discretion, keep the records for a longer period of time if it is deemed necessary and appropriate, and where it is required for a specific purpose (e.g. the defence of litigation).

3.4. A list of the vital records held within Kerry ETB, shall be prepared and reviewed periodically. For example, Board/Committee meetings, Sub-committee meetings, Board of Management meetings, financial information, legal documentation etc. should be included in this. It is recommended that vital records be duplicated with one set being stored on site and the other off site in case of a disaster such as fire.

4. Employee Duties

4.1. All Kerry ETB employees are responsible for making and keeping the records of their work and shall:

4.1.1. Comply with the "Filing Guidelines" set out at Appendix 1 hereto.

4.1.2. Create records needed to do the business of Kerry ETB, record decisions and actions taken, and generally document activities for which they are responsible and take care of records so that information can be found when needed. This means establishing or adhering to good directories and files, and filing materials (in any format) regularly and carefully in a manner that allows them to be safely stored and efficiently retrieved and returned when necessary.

4.1.3. Ensure that all records under their control are stored/retained/destroyed or archived in accordance with Kerry ETB's Records Retention Schedule (see Appendix 4 of Kerry ETB Data Protection Policy).

5. Retention and Disposal

5.1. After the records have been retained by the creating/receiving department/ office/school/institute/centre (in-situ or off-site storage) for the requisite time in the Record Retention Schedule, they are either securely destroyed (e.g. by confidential cross-shredding by a third party contractor retained pursuant to a Data Processing Agreement as required by the Data Protection Policy of Kerry ETB), or securely transferred to archival storage.

5.2. It is the responsibility of the Principal/Director/Co-ordinator/Head of Section to ensure that records are scheduled as necessary to be retained in the appropriate storage facility or securely disposed of.

5.3. If a file is to be destroyed, then a Destruction Record Form needs to be completed by the employee and countersigned by the senior member of staff responsible for records destruction. The Destruction Record Form shall be filed and kept permanently.

5.4. A Destruction Register must be created and maintained by each administrative department/school/institute centre/programme under the remit of Kerry ETB which contains all the completed Destruction Record Forms.

6. Life-Cycle of Records within the ETB

6.1. Each record has a Life Cycle, which is as follows:

Current Records	Are those that are held on site in offices and are used on a very regular basis.
Non-current Records	These are records that are needed for occasional reference. Can be held on site in a dedicated storage area or stored off site with easy access.
Disposition	Records which should either be archived or securely and confidentially cross-shredded.

6.2. **Current Records:**

6.2.1. Active Records: Active records are records that are required and referred to constantly for current use, and which need to be retained and maintained in office space and equipment close and readily accessible to users.

6.2.2. Semi-active Records: Semi-active records are records that are referred to infrequently and are not required constantly for current use. Semi-active records are removed from office space to storage until they are no longer needed.

6.3. **Non-Current Records**

6.3.1. Inactive Records: Inactive records are records which are no longer required to carry out the functions for which they were created. They should be stored until the retention period has lapsed.

6.3.2. Permanently Valuable Records – Archives: Permanently valuable records include those with legal, operational, administrative, historical, scientific, cultural and social significance.

APPENDIX 1: Filing Guidelines

a) Before filing a piece of paper, ask yourself, "Will I need this in the future?" Don't keep a piece of paper just on the chance that you may need it "someday."

b) Don't always save every draft of a document. For most purposes the final version is sufficient.

c) Don't file multiple copies of the same document, unless justified.

d) The originator normally keeps copies of reports and correspondence. Just because a document is sent to you does not mean that you are obliged to keep it indefinitely. If you need to see it again, ask the originator for another copy.

e) If, for example, records are scheduled for destruction after three years, don't store them for five years.

f) In general, records received from ETB schools/institutes/centres/offices should be filed under the name of the originating school/institute/centre/office.

g) Some records may belong under more than one series or category. To handle this, file the records in one category and place a cross-reference note in the other. It is important to be consistent in deciding where to file records. Once information is filed in a given series and category, it should always be filed there.

h) Label and date all files.

i) Color-coding the different series is a useful tool, especially for refiling folders.

j) Create a file guide with a description of the filing system and instructions for the user so new personnel can continue to use the filing system easily. This will also avoid the arbitrary creation of new file folders.

k) Create cross-listings to help locate items. Create a file database on the PC using the file-folder heading, cross-listing, and location notes.

l) Spell out acronyms and abbreviations.

m) Sort records prior to filing.

n) Use staples rather than paper clips in folders.

o) Discard envelopes if the return address is available on the document itself. Most phone messages, illegible notes, and routine acknowledgements can also be discarded.

p) Do not overfill file folders. If they are overfilled, divide them into several folders with the same name and File number (e.g.: Maternity Leave Applications 2008/2009, File 1).

q) Do not overstuff file drawers. This can make retrieval of files difficult, as well as creating a dangerous work environment.

r) Weed files regularly, using the approved Record Retention Schedule.

s) Consider using "Out Markers" when removing folders for use. This makes refiling much easier and lets others in the office know that a file exists so another is not created, who has the file, and when it was checked out.

Appendix 4
Kerry ETB Record Retention Schedule

Records Retention Schedule

Retention of Records

Schools and ETBs 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, *<Named school/ETB>* 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/ETB 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

Records Retention Schedule

Student Records	Primary	Vol Sec.	C&C	ETB	Final disposition	Comments
Registers/Roll books	Indefinitely	Indefinitely	Indefinitely	Indefinitely	N/A	Indefinitely. Archive when class leaves + 2 years
State exam results	N/A	N/A	N/A	N/A	N/A	SEC responsibility to retain, not a requirement for school/ETB to retain.

Records relating to pupils/students	Primary	Vol.Sec	C&C	ETB	Confidential shredding	Comments
Enrolment Forms	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	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)
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	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	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)
Disciplinary notes	Never destroy	Never destroy	Never destroy	Never destroy	N/A	Never destroy
Results of in-school tests/exams (i.e. end of term, end of year exams, assessment results)	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	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).
End of term/year reports	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	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)
Records of school tours/trips, including permission slips, itinerary reports	Never destroy	Never destroy	Never destroy	Never destroy	N/A	Never destroy

Records relating to pupils/students	Primary	Vol.Sec	C&C	ETB	Confidential shredding	Comments
Scholarship applications e.g. Gaeltacht, book rental scheme	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	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)
Garda vetting form & outcome - **STUDENTS**	N/A as **primary schools pupils will not be undergoing vetting**	Record of outcome retained for 12 months.	Record of outcome retained for 12 months.	Record of outcome retained for 12 months.	Confidential shredding	Record of outcome retained for 12 months. School to retain the reference number and date of disclosure on file, which can be checked with An Garda Siochana in the future.

Sensitive Personal Data Students	Primary	Vol Sec.	C&C	ETB	Final disposition	Comments
Psychological assessments	Indefinitely	Indefinitely	Indefinitely	Indefinitely	N/A - Never destroy	Never destroy
Special Education Needs' files, reviews, correspondence and Individual Education Plans	Indefinitely	Indefinitely	Indefinitely	Indefinitely	N/A	Never destroy
Accident reports	Indefinitely	Indefinitely	Indefinitely	Indefinitely	N/A	Never destroy
Child protection records	Indefinitely	Indefinitely	Indefinitely	Indefinitely	N/A	Never destroy
Section 29 appeal records	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	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)
Enrolment/transfer forms where child is not enrolled or refused enrolment	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Student reaching 18 years + 7 years	Confidential shredding	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)

Sensitive Personal Data Students	Primary	Vol Sec.	C&C	ETB	Final disposition	Comments
Records of complaints made by parents/ guardians	Depends entirely on the nature of the complaint.	Depends entirely on the nature of the complaint.	Depends entirely on the nature of the complaint.	Depends entirely on the nature of the complaint.	Confidential shredding or N/A, depending on the nature of the records.	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)

Staff Records	Primary	Vol Sec.	C&C	ETB	Final disposition	Comments
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.	✓	✓	✓	✓ **Note:** Recruitment and employment records are held at ETB Head Office in the HR and Finance Depts.	Confidential shredding	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.
Applications & CVs of candidates called for interview	✓	✓	✓	✓	Confidential shredding	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.
Database of applications	✓	✓	✓	✓	Confidential shredding	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.

Staff Records	Primary	Vol Sec.	C&C	ETB	Final disposition	Comments
Selection criteria	✓	✓	✓	✓	Confidential shredding	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.
Applications of candidates not shortlisted	✓	✓	✓	✓	Confidential shredding	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.
Unsolicited applications for jobs	✓	✓	✓	✓	Confidential shredding	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.
Candidates shortlisted but unsuccessful at interview	✓	✓	✓	✓	Confidential shredding	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.
Candidates shortlisted and are successful but do not accept offer	✓	✓	✓	✓	Confidential shredding	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.
Interview board marking scheme & board notes	✓	✓	✓	✓	Confidential shredding	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.
Panel recommendation by interview board	✓	✓	✓	✓	Confidential shredding	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.

Staff personnel files (whilst in employment)	**Primary**	**Vol.Sec**	**C&C**	**ETB**	**Final Disposition**	**Comments**
e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, records of staff training etc.				Note: records & personnel files retained at ETB head office level	Confidential shredding. Retain an anonymised sample for archival purposes.	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)
Application &/CV	✓	✓	✓	✓	Confidential shredding	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)
Qualifications	✓	✓	✓	✓	Confidential shredding	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)
References	✓	✓	✓	✓	Confidential shredding	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)
Interview: database of applications (the section which relates to the employee only)	✓	✓	✓	✓	Confidential shredding	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)
Selection criteria	✓	✓	✓	✓	Confidential shredding	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)
Interview board marking scheme & board notes	✓	✓	✓	✓	Confidential shredding	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)
Panel recommendation by interview board	✓	✓	✓	✓	Confidential shredding	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)

Staff personnel files (whilst in employment)	Primary	Vol.Sec	C&C	ETB	Final Disposition	Comments
Recruitment medical	✓	✓	✓	✓	Confidential shredding	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)
Job specification/ description	✓	✓	✓	✓	Confidential shredding	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)
Contract/Conditions of employment	✓	✓	✓	✓	Confidential shredding	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)
Probation letters/forms	✓	✓	✓	✓	Confidential shredding	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)
POR applications and correspondence (whether successful or not)	✓	✓	✓	✓	Confidential shredding	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)
Leave of absence applications				Records & personnel files retained at ETB head office level	Confidential shredding	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)
Job share	✓	✓	✓	✓	Confidential shredding	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)
Career Break	✓	✓	✓	✓	Confidential shredding	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)
Maternity leave	✓	✓	✓	✓	Confidential shredding	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)

Staff personnel files (whilst in employment)	Primary	Vol.Sec	C&C	ETB	Final Disposition	Comments
Paternity leave	✓	✓	✓	✓	Confidential shredding	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).
Parental leave	✓	✓	✓	✓	Confidential shredding	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). There is a statutory requirement to retain for 8 years.
Force Majeure leave	✓	✓	✓	✓	Confidential shredding	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.
Carers leave	✓	✓	✓	✓	Confidential shredding	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
Working Time Act (attendance hours, holidays, breaks)	✓	✓	✓	✓	Confidential shredding	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
Allegations/complaints	✓	✓	✓	✓	ETB one doesn't have a time period advised	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.
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	Vol Sec.	C&C	ETB	Confidential Shredding	Comments
Sickness absence records/certificates	✓	✓	✓	Retain on staff personnel file at ETB HO	Confidential shredding Or do not destroy.	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.
Pre-employment medical assessment	✓	✓	✓	✓	Confidential shredding Or do not destroy?	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.
Occupational health referral	✓	✓	✓	✓	Confidential shredding Or Do not destroy.	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.
Correspondence re retirement on ill-health grounds	✓	✓	✓	✓	Confidential shredding Or Do not destroy.	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.
Accident/injury at work reports	✓	✓	✓	✓	Confidential shredding	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).
Medical assessments or referrals	✓	✓	✓	✓	Confidential shredding Or Do not destroy.	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.
Sick leave records (sick benefit forms)	✓	✓	✓	✓	Confidential shredding	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)

Superannuation /Pension /Retirement records	Primary	Vol Sec.	C&C	ETB	Final Disposition	Comments
Records of previous service (incl. correspondence with previous employers)	✓	✓	✓	Superannuation records are held at ETB head office in the HR and Finance Depts.	N/A	DES advise that these should be kept indefinitely.
Pension calculation	✓	✓	✓	✓	Confidential shredding	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)
Pension increases (notification to Co. Co.)	✓	✓	✓	✓	Confidential shredding	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)
Salary claim forms	✓	✓	✓	✓	Confidential shredding	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)

Government returns	Primary	Vol Sec.	C&C	ETB	Final disposition	Comments
Any returns which identify individual staff/pupils,				Submitted online to DES. Printout retained by ETB HO	N/A	**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.**

Board of Management Records	Primary	Vol Sec.	C&C	ETB	Final disposition	Comments
Board agenda and minutes	✓	✓	✓	Sent to ETB for approval	N/A	Indefinitely. These should be stored securely on school property
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	Vol Sec.	C&C	ETB	Final disposition	Comments
CCTV recordings	✓	✓	✓	✓	Safe/secure deletion.	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.
Principal's monthly report including staff absences	✓	✓	✓	Submitted to ETB HO	N/A	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".

Financial Records	Primary	Vol Sec.	C&C	ETB	Final disposition	Comments
Audited Accounts	✓	✓	✓	Retained ETB head office	n/a	Indefinitely
Payroll and taxation	✓	✓	✓	Retained ETB head office		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	Vol Sec.	C&C	ETB Employment records are held at ETB head office in the HR and Finance Depts.	**Final Disposition**	**Comments**
Posts of Responsibility	✓	✓	✓		N/A	**Retain indefinitely on master file as it relates to pay/pension etc. (See DES guidelines)**
Calculation of service	✓	✓	✓		N/A	Retain indefinitely on master file
Promotions/POR Board master files	✓	✓	✓		N/A	Retain indefinitely on master file
Promotions/POR Boards assessment report files	✓	✓	✓		N/A	Retain original on personnel file in line with retention periods in "Staff Records" retention guidelines above
POR appeal documents	✓	✓	✓		N/A	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.
Correspondence from candidates re feedback	✓	✓	✓		N/A	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.

Appendix 5
Kerry ETB Personal Data Rectification/Erasure Form

BORD OIDEACHAIS AGUS OILIÚNA CHIARRAÍ
KERRY EDUCATION AND TRAINING BOARD

Date:

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 (e.g. official/State photographic identity document such as drivers licence, passport) must accompany this form.

Full Name	
Address	
Contact number *	Email addresses *

* Kerry ETB 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: Yeargroup/class:	Name of Student:	Insert Year of leaving:		Insert Years From/To:

I, ...[insert name] wish to have the data detailed below which Kerry ETB 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 Kerry 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 (drivers licence, Passport etc.)*. ☐

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

Please return this form to: **<Insert name of officer in charge of handling these request>** ***<insert address >***

Appendix 6

BORD OIDEACHAIS AGUS OILIÚNA CHIARRAÍ
KERRY EDUCATION AND TRAINING BOARD

Data Access Procedures Policy

Date of adoption by Kerry ETB: *27th April, 2015*

The Data Protection Acts, 1988 and 2003 provide for a right of access by an individual data subject to personal information held by *Kerry ETB.* The following procedure is provided to ensure compliance with the ETB's obligations under the Acts and governs the manner in which requests for access to personal data will be managed by Kerry ETB. A data subject is required to familiarize themselves with the procedure and to complete the **Data Access Request Form** (see Appendix 7 of the Data Protection Policy) which will assist the ETB in processing the access request where personal information (or in the case of a parent/guardian making an access request on behalf of a student, personal information in relation to their child) as a data subject is processed and retained by *Kerry ETB.* It is important to note that only personal information relating to the individual (or in the case of a parent/guardian making an access request on behalf of a student, only personal information in relation to his/her/their child) will be supplied. No information will be supplied that relates to another individual.

Important note to students making access requests

Where a student (aged under 18 years) makes an access request, Kerry ETB may inform the student that:

(a) Where they make an access request, their parents will be informed that they have done so and

(b) A complete copy of the access request materials being furnished to the data subject by Kerry ETB will also be furnished to the student's parent/guardian.

This is provided for in Kerry ETB's Data Protection Policy. The right of access under the Data Protection Acts is the right of the data subject. However, there may be some data held by Kerry ETB which may be of a sensitive nature and Kerry ETB will have regard to the following guidance issued by the Office of the Data Protection Commissioner in relation to releasing such data:

a) A student aged **eighteen years or older** (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.

b) If a student aged **eighteen years or older** has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.

c) A student aged from **twelve up to and including seventeen** can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is suggested that:

- If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
- If the information is of a sensitive nature, it would be prudent to seek parental/guardian consent before releasing the data to the student

- If the information would be likely to be harmful to the individual concerned, parental/guardian consent should be sought before releasing the data to the student.

d) In the case of students under the age of twelve, an access request may be made by their parent or guardian on the student's behalf. However, Kerry ETB must note that the right of access is a right of the data subject themselves (i.e. it is the right of the student). Therefore, access documentation should be addressed to the child at his/her address which is registered with the school as being his/her home address. It should not be addressed or sent to the parent who made the request. For further information, see "Important Note to Parents Making Access Requests on Behalf of their Child" below.

Important note to parents making access requests on behalf of their child

Where a parent/guardian makes an access request on behalf of their child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the child, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the child is registered on the school's records and will be addressed to the child. The documentation will not be sent to or addressed to the parent/guardian who made the request. Where a parent/guardian is unhappy with this arrangement, the parent/guardian is invited to make an application to court under section 11 of the Guardianship of Infants Act 1964. This provision enables the court (on application by a guardian) to make a direction on any question affecting the welfare of the child. Where a court issues an order stating that a school should make certain information available to a parent/guardian, a copy of the order should be given to the school by the parent/guardian and the school can release the data on foot of the court order.

Individuals making an access request

On making an access request, any individual (subject to the restrictions in Notes A and B below) about whom Kerry ETB keeps *Personal Data*, is entitled to:

- a copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts apply, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
- know the purpose/s for processing his/her data
- know the identity (or the categories) of those to whom the data is disclosed
- know the source of the data, unless it is contrary to public interest
- where the processing is by automated means (e.g. credit scoring in financial institutions where a computer program makes the "decision" as to whether a loan should be made to an individual based on his/her credit rating) know the logic involved in automated decisions.

Data access requirements

To make an access request, you as a data subject must:

1. Apply in writing requesting access to your data under section 4 Data Protection Acts or, alternatively, request an Access Request Form (see Appendix 7 of the Data Protection Policy) which will greatly assist Kerry ETB in processing your access request more quickly. In the

case of Kerry ETB schools, correspondence should be addressed in the first instance to the school principal (save where personnel files or other files are retained by Kerry ETB head office – in such circumstances correspondence should be addressed to the Chief Executive Officer of Kerry ETB)

2. You will be provided with a form which will assist Kerry ETB in locating all relevant information that is held subject to the exceptions and prohibitions outlined in **Appendix A.** The school reserves the **right to request official proof of identity** (e.g. photographic identification such as a passport or driver's licence) where there is any doubt on the issue of identification.
3. On receipt of the access request form, a co-ordinator will be appointed to check the validity of your access request and to check that sufficient information to locate the data requested has been supplied (particularly if CCTV footage/images are to be searched). In the case of Kerry ETB schools, the co-ordinator is the Chief Executive of Kerry ETB. It may be necessary for the co-ordinator to contact you in the event that further details are required with a view to processing your access request.
4. The co-ordinator will log the date of receipt of the valid request and keep a note of all steps taken to locate and collate the requested data.
5. The co-ordinator will ensure that all relevant manual files (held within a "relevant filing system") and computers are checked for the data in respect of which the access request is made.
6. The co-ordinator will ensure that the information is supplied promptly and within the advised timeframes in items 7, 8 and 9 as appropriate.
7. **Where a request is made under Section 3 of the Data Protection Acts,** the following information will be supplied: (i) what Kerry ETB holds by way of personal information about you ((or in the case of a request under section 3 made by a parent/guardian of a student aged under 18 years, then the personal information held about that student) and (ii) a **description** of the data together with details of the purposes for which his/her data is being kept will be provided. Actual copies of your personal files (or the personal files relating to the student) will not be supplied. No personal data can be supplied relating to another individual. A response to your request will be provided within 21 days of receipt of the access request form and no fee will apply.
8. **Where a request is made under Section 4 of the Data Protection Acts,** the following information will be supplied within **40 days and an administration fee of €6.35 will apply.** The individual is entitled to a copy of all personal data, i.e.
    - A copy of the data which is kept about him/her (unless one of the exemptions or prohibitions under the Data Protection Acts applies, in which case the individual will be notified of this and informed of their right to make a complaint to the Data Protection Commissioner)
    - Be advised of the purpose/s for processing his/her data
    - Be advised of the identity (or the categories) of those to whom the data is disclosed
    - Be advised of the source of the data, unless it is contrary to public interest
    - Where the processing is by automated means (e.g. credit scoring in financial institutions where a computer program makes the "decision" as to whether a loan should be made to an individual based on his/her credit rating), know the logic involved in automated decisions.

9. Where a request is made with respect to **examination results** an increased time limit of **60 days** from the date of the first publication of the results or from the date of the access request, whichever is the later will apply.

10. Before supplying the information requested to you as data subject (or where the access request is made on behalf of a student aged under 18 years, information relating to the student), the co-ordinator will check each item of data to establish:
    - If any of the exemptions or restrictions set out under the Data Protection Acts apply, which would result in that item of data not being released, or
    - where the data is "health data", whether the obligation to consult with the data subject's medical practitioner applies, or
    - where the data is "social work data", whether the prohibition on release applies.

11. If data relating to a third party is involved, it will not be disclosed without the consent of that third party or alternatively the data will be anonymised in order to conceal the identity of the third party. Where it is not possible to anonymise the data to ensure that the third party is not identified, then that item of data may not be released.

12. Where an ETB may be unsure as to what information to disclose, Kerry ETB reserves the right to seek legal advice.

13. The co-ordinator will ensure that the information is provided in an intelligible form (e.g. codes explained) or will provide an explanation.

14. Number the documents supplied.

15. Have the response "signed-off" by an appropriate person. In the case of Kerry ETB schools, this function is undertaken by the Chief Executive of the Kerry ETB/nominee.

16. Kerry ETB will respond to your access request within the advised timeframes contingent on the type of request made.

17. Kerry ETB reserves the right to supply personal information to an individual in an electronic format e.g. on tape, USB, CD etc.

18. Where a subsequent or similar access request is made after the first request has been complied with, Kerry ETB has discretion as to what constitutes a reasonable interval between access requests and this will be assessed on a case-by case basis.

19. Where you as an individual data subject may seek to rectify incorrect information maintained by Kerry ETB, please notify Kerry ETB and a form will be supplied to you for this purpose. You should however note that the right to rectify or delete personal data is not absolute. You have the right to make a complaint to the Data Protection Commissioner about a refusal. Where Kerry ETB declines to rectify or delete the personal data as you have instructed, Kerry ETB may propose to supplement your personal record, pursuant to section 6(1)(b) Data Protection Acts.

20. In circumstances where your access request is refused, Kerry ETB will write to you explaining the reasons for the refusal and the administration fee, if provided, will be returned. In such circumstances, you have the right to make a complaint to the Office of the Data Protection Commissioner www.dataprotection.ie. Similarly, the administration access fee will be refunded to you if the ETB has to rectify, supplement or erase your personal data.

21. **Where requests are made for CCTV footage,** an application must be made in writing and the timeframe for response is within 40 days. All necessary information such as the date, time and location of the recording should be given to Kerry ETB to assist Kerry ETB in dealing with your request. Where the image is of such poor quality as not to clearly identify an individual,

that image may not be considered to be personal data. In providing a copy of personal data, Kerry ETB may provide the materials in the form of a still/series of still pictures, a tape, disk, USB, with relevant images. Other people's images will be obscured before the data is released. If other people's images cannot be obscured, then the images/recordings may not be released.

There are a number of exceptions to the general rule of right of access, including those specified in Notes A and B in **Appendix A.**

This procedure is regularly reviewed in line with Kerry ETB's commitment to its responsibilities under data protection.

Note A: Access requests by students

- A student aged **eighteen years or older** (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves.
- If a student aged **eighteen years or older** has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student.
- A student aged from **twelve up to and including seventeen** can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is suggested that
- If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
- If the information is of a sensitive nature, it would be prudent to seek parental/guardian consent in writing before releasing the data to the student. Where the parent/guardian does not give their consent to releasing the data to the student, legal advice should be sought
- If the information would be likely to be harmful to the individual concerned, parental/guardian consent should be sought before releasing the data to the student.
- In the case of students **under the age of twelve**, an access request may be made by their parent or guardian on the student's behalf. The consent of the child need not be obtained. However, Kerry ETB must note that the right of access is a right of the data subject themselves (i.e. it is the right of the student). Therefore, access documentation should be addressed to the child at his/her address which is registered with the school as being his/her home address. **It should not be addressed or sent to the parent who made the request.** For further information, see "Important Note to Parents Making Access Requests on Behalf of their Child" below.
- In any of the circumstances outlined above, if the data contains health data and disclosure would be likely to cause serious harm to the physical or mental health of the individual concerned, Kerry ETB is obliged to withhold the data until they have consulted with the data subject's medical practitioner and (in the case of a student under 18 or a student with special educational needs whose disability or medical condition would impair his or her ability to understand the information), parental/guardian consent should also be sought.
- In some cases (i.e. where the information is "**health data**"), it is advised that the data be supplied by the medical practitioner.
- In any of the circumstances outlined above, if the data contains **social work data** and disclosure would be likely to cause serious harm to the physical or mental health of the individual, Kerry ETB is not permitted to release the data to the individual.

Note B: Exceptions to note:
Data protection regulations **prohibit** the supply of:

- **Health data** to a patient in response to a request for access if that would be likely to cause serious harm to his or her physical or mental health. This is to protect the individual from hearing anything about himself or herself which would be likely to cause serious harm to their physical or mental health or emotional well-being. In the case of health data, the information can only be released after the Kerry ETB has consulted with the appropriate health professional (usually the data subject's GP).

- *Personal Data* obtained in the course of carrying on social work (**"social work data"**) (personal data kept for or obtained in the course of carrying out social work by a Government department, local authority, TUSLA etc) is also restricted in some circumstances if that would be likely to cause serious harm to the health or emotional condition of the data subject concerned. In the case of social work data, the information cannot be supplied at all if Kerry ETB believes it would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject. If the social work data includes information supplied to Kerry ETB by an individual (other than one of Kerry ETB's employees or agents) while carrying out social work, Kerry ETB is not permitted to supply that information to the data subject without first consulting that individual who supplied the information.

The Data Protection Acts state that the following data is **exempt** from a data access request:

1. Section 5 of the Data Protection Act provides that the right of access does not apply in a number of cases in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society on the other hand. Examples would include the need for state agencies (like An Garda Síochána) to **investigate crime** effectively and the need to protect the international relations of the State.
2. **Estimates of liability**: where the personal data consists of or is kept for the purpose of estimating the amount of the liability of Kerry ETB on foot of a claim for damages or compensation and where releasing the estimate would be likely to prejudice the interests of Kerry ETB in relation to the claim, the data may be withheld.
3. **Legally privileged information**: the general rule is that all documentation prepared in contemplation of litigation is legally privileged. So correspondence between Kerry ETB and their solicitors/legal advisors in relation to a case against Kerry ETB should not be disclosed to the claimant pursuant to a data access request.
4. Section 4 states that the right of access does not include a right to see **personal data about another individual**, without that other person's consent. This is necessary to protect the privacy rights of the other person. If it is reasonable for Kerry ETB to conclude that redacting or omitting the particulars identifying the third party would both conceal the identity of the third party and enable the data to be disclosed (subject to the redactions), then the data could be disclosed with such redactions. However, if it is not possible to redact or omit the particulars which identify a third party, then the affected data should not be released to the applicant.

5. Section 4 also states that where personal data consists of **expressions of opinion** about the data subject made by another person, the data subject has a right to receive that expression of opinion **except** where that expression of opinion was given in confidence, and on the clear understanding that it would be treated as confidential.
6. The obligation to comply with an access request does not apply where it is impossible for Kerry ETB to provide the data or where it involves a disproportionate effort.

Where Kerry ETB refuses to hand over some or all of the personal data they hold in relation to a data subject (on the basis of any of the exemptions or prohibitions set out above), Kerry ETB must advise the data subject of this in writing, setting out reasons for the refusal and notifying the data subject that he or she has the right to complain to the Office of the Data Protection Commissioner about the refusal. For further information, see

What if a school/ETB refuses an access request?

Where a school/ETB refuses an access request (or refuses to hand over all the data which they hold in relation to a data subject), the school/Kerry ETB must write to the individual explaining the reasons for the refusal (i.e.setting out the exemptions/prohibitions upon which it is relying for not furnishing the data, and notifying the individual that they may complain to the Data Protection Commissioner about the refusal.

BORD OIDEACHAIS AGUS OILIÚNA CHIARRAÍ
KERRY EDUCATION AND TRAINING BOARD

Appendix 7
Data Access Request Form

Date:

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

<u>Important:</u> 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 *(if name used during* your school duration*)*	
Address	
Contact number *	Email addresses *

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

Please tick the box which applies to you:

Student ☐	Parent/Guardian of student ☐	Former Student ☐	Current Staff ☐	Former Staff ☐
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 *<Kerry ETB>* 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

BORD OIDEACHAIS AGUS OILIÚNA CHIARRAÍ
KERRY EDUCATION AND TRAINING BOARD

Section 4 Data Access Request:

I, ... [insert name] wish to make an access request for a copy of any personal data that Kerry ETB 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 enclose €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 ETB to locate the data).

Signed ..... Date .....

Checklist: Have you:

1) Completed the Access Request Form in full? ☐
2) Included a cheque or postal order made payable to *Kerry ETB* 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). ☐
3) Signed and dated the Access Request Form? ☐
4) Included a photocopy of official/State photographic identity document (driver's licence, passport etc.)*. ☐

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

Please return this form to: ***Chief Executive Officer, Kerry ETB, Centrepoint, John Joe Sheehy Road, Tralee, Co. Kerry***