CEIST

Catholic Education
An Irish Schools Trust

CEIST **CLG**

Data Protection Policy

Date: __22/8/2019_____

Catholic Education
An Irish Schools Trust

Table of Contents

Section 1: CEIST Data Protection Policy

1.1 Introduction:

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of CEIST. This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish and EU legislation, namely the General Data Protection Act (GDPR) 2018, and the Irish Data Protection Acts 1988 to 2018.

1.2 Rationale:

CEIST must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by CEIST in relation to its staff, schools, community schools, service providers and wider members of the CEIST community in the course of its activities. CEIST makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

1.3 Scope:

The policy covers both personal and sensitive personal data held in relation to data subjects by CEIST. The policy applies equally to personal data held in manual and automated form. All Personal and Sensitive Personal Data will be treated with equal care by CEIST. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Subject Access Request procedure, Data Retention and Destruction policy, Privacy Statement and Data Loss Notification procedure.

1.4 CEIST as a Data Controller

In the course of its daily organisational activities, CEIST acquires, processes and stores personal data in relation to:

- Employees of CEIST
- Schools that are under CEIST Trusteeship
- Staff and Board of Management Members within schools under CEIST Trusteeship
- Community schools for which CEIST carries out a Trusteeship role on behalf of its congregations
- Staff and Board of Management Members within community schools for which CEIST carries out a Trusteeship role on behalf of its congregations
- Third party service providers engaged by CEIST
- Members of CEIST
- Board of Directors of CEIST

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. Not all CEIST staff members will be expected to be experts in Data Protection legislation.

However, CEIST is committed to ensuring that its staff has sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the **Information Communications Technology (ICT) Coordinator** in his/her capacity as Data Protection Officer is informed, in order that appropriate corrective action is taken.

Due to the nature of the services provided by CEIST, there is regular and active exchange of personal data between CEIST and its Data Subjects. In addition, CEIST exchanges personal data with Data Processors on the Data Subjects' behalf. This is consistent with the obligations of CEIST under the terms of its contract with its Data Processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow if a CEIST staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

1.5 Third-Party Processors

In the course of its role as Data Controller, CEIST engages a number of Data Processors to process Personal Data on its behalf. In each case, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish and EU Data Protection legislation.

1.6 Implementation

As a Data Controller, CEIST ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation. Failure of a Data Processor to manage data of CEIST in a compliant manner will be viewed as a breach of contract and will be pursued through the courts. A written contract (or a contract in another equivalent form) is required where a Data Controller engages the services of a Data Processor (outside person / organisation / company). The contract must provide that the Data Processor:

- carries out the processing only subject to the instructions of the Data Controller and provides appropriate security measures;
- provides sufficient guarantees in respect of the technical and organisational security measures, and
- takes reasonable steps to ensure compliance with those measures.

Informal or ad hoc arrangements between Data Controllers and Data Processors are not acceptable.

Failure of CEIST staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

1.7 Fair Processing of Personal Data

In order to be seen to have processed the data fairly CEIST must make the following available to the data subject at the time of obtaining the data:

1. the identity of the Data Controller, or of his/her representative;
2. purpose(s) for which the data are intended to be processed, and
3. any other information so that the processing will be fair to the data subject, such as, recipients of the data, whether questions used in the collection of the data are obligatory, possible consequences of failure to give such replies, the existence of the right of access and rectification available to the data subject.

In any other case the Data Controller must make the above information available to the data subject not later than the first time the data is processed, or if the disclosure of the data to a third party is envisaged, before it is disclosed. The categories of data concerned, and the name of the original Data Controller must also be given to the data subject in this circumstance. However, this is not required if the processing is for statistical, historical, or scientific research, where to provide the information would require a disproportionate effort or be impossible, or the processing is required by legal obligation.

1.8 The Data Protection Principals

The following key principles are enshrined in the Irish legislation and are fundamental to the Data Protection Policy of CEIST. In its capacity as Data Controller, CEIST ensures that all data shall:

1. Be obtained and processed fairly and lawfully.
The data or the information constituting the data must be obtained and processed fairly. All individuals for which data is collected should be told why the information is needed and be given an explanation of what use may be made of such information. The information should not be used for any other purpose. For data to be obtained fairly, the data subject will, at the time the data is being collected, be made aware of:

- The identity of the Data Controller (CEIST).
- The purpose(s) for which the data is being collected.
- The person(s) to whom the data may be disclosed by the Data Controller.
- Any other information that is necessary so that the processing may be fair.

CEIST will meet this obligation in the following way:

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, CEIST will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where CEIST intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;
- Processing of the personal data will be carried out only as part of the lawful activities of CEIST, and CEIST will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to CEIST and operating on its behalf.

2. Be obtained only for one or more specified, explicit and legitimate purposes.
The data shall be obtained for one or more specified, explicit and legitimate purpose(s). This means that if the data is kept for other purposes, a complaint to, and an investigation by, the Data Protection Commissioner may result in prosecution under the Act. CEIST will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which CEIST holds their data, and CEIST will be able to clearly state that purpose or purposes.

3. Not be further processed in a manner incompatible with the specified purpose(s).
Any use of the data by CEIST will be compatible with the purposes for which the data was acquired. The data shall not be further processed in a manner incompatible with those purposes.

4. Be kept safe and secure.
CEIST will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by CEIST in its capacity as Data Controller. Access to and management of staff and school data is limited to those staff members who have appropriate authorisation and password access.

5. Be kept accurate, complete and up-to-date where necessary.
The data should be accurate and complete, and kept up to date. CEIST will meet this obligation in the following way:

- Ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. CEIST conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years.
- Conduct regular assessments in order to establish the need to keep certain Personal Data.

6. Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.
The data shall be adequate, relevant and not excessive in relation to that purpose(s), for which they were collected or are further processed. In other words, the data kept must be in proportion to the use which they are put. CEIST will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. Not be kept for longer than is necessary to satisfy the specified purpose(s).
The data shall not be kept for longer than is necessary. At some stage, data will become stale or irrelevant and should no longer be kept. CEIST has identified data categories, with reference to the appropriate data retention period for each category. This applies to data in both a manual and automated format. Once the respective retention period has elapsed, CEIST undertakes to archive, destroy, erase or otherwise put this data beyond use depending on the category of data. See the "CEIST Data Retention and Destruction Policy" for full details.

8. Give a copy of his/her personal data to an individual, on request.
CEIST has implemented a "Subject Access Request" procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

1.9 Data Subject Access Request

Right of Access

As part of the day-to-day operation of the organisation, CEIST's staff engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by CEIST, such a request gives rise to access rights in favour of the Data Subject.
The individual is entitled, on foot of a written request, to be:

- informed by CEIST of any personal data relating to him/her;
- supplied with a description of the categories of data being processed, what personal data relates to him/her, the purposes(s) of the processing, and the recipients to whom the data have or may be disclosed to;
- supplied with a copy of the information, in a permanent form, and any information CEIST has as to the source of the data;

If any of the information is expressed in terms that are not intelligible to the average person, the information must be accompanied by an explanation. The data subject should be given a copy of the information unless supplying a copy is not possible, or would involve disproportionate effort, or the data subject agrees otherwise. CEIST has one calendar month within which to comply with such a request.

Proof of Identity

The individual making the access request must provide CEIST with:

- Proof of identity, and
- Reasonable information to locate any relevant personal data

CEIST is not obliged to disclose a data subject personal data referring to another individual, without his/her consent.

Data Expressing Opinions

Where the personal data consist of an expression of opinion about the data subject by another person, the data can be disclosed to the data subject without the permission of that other person. This however, does not apply to personal data where an opinion was given in confidence.

Restriction of Right of Access

Both GDPR and The Irish Data Protection Act 2018 allow for an individual's rights to be restricted in certain circumstances, for example if data held by CEIST relates to a legal case. Full information regarding access restrictions can be found in Article 23 of GDPR and Sections 59-61 of the Irish Data Protection Act 2018.

Access Fee

CEIST will not charge any fee for data access requests.

Subsequent Requests

If CCIST has previously complied with a request, CCIST is not obliged to comply with a subsequent request from the same individual, unless, in the Data Controller's opinion a reasonable interval has elapsed. Regard must be had to the nature of the data, the purpose for which they are being processed, and the frequency with which they are altered.

Refusal to Comply with a Request

A refusal by CCIST to comply with a request for access must be in writing, with a statement of the reasons for the refusal, and an indication that a complaint can be made to the Data Protection Commissioner.

1.10 Data Breach

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner within 72 hours of breach occurring. The only exceptions to this policy are when the data subjects have already been informed, and where the loss involves only non-sensitive, non-financial personal data. Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commissioner is notified only where the data on such devices is not encrypted. See "Data Loss Notification Procedure" for full details.

1.11 Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data

This includes both automated and manual data.
Automated data means data held on computer or stored with the intention that it is processed on computer.
Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.

Personal Data

Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, CCIST refers to the definition issued by the Article 29 Working Party and updated from time to time.)

Sensitive Personal Data

A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.

Data Controller
A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.

Data Subject
A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.

Data Processor
A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.

Data Protection Officer
A person appointed by CCIST to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients.

Relevant Filing System
Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.

Section 2: CEIST Data Retention and Destruction Policy

2.1 Purpose

The purpose of this Policy is to ensure that necessary hard copy documents of the company are adequately protected and maintained and to ensure that documentation that are no longer needed by CEIST and/or of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of CEIST in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

2.2 Policy

This Policy represents CEIST policy regarding the retention and disposal of hard copy documentation and the retention and disposal of electronic documents.

2.3 Administration

The Record Retention Schedule included towards the end of this document is approved as the initial maintenance, retention and disposal schedule for physical records of CEIST and the retention and disposal of electronic documents. The CEIST ICT Coordinator is the Data Protection Officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed.

2.4 Applicability

This Policy applies to all physical records generated in the course of the Trusts operation, including both original documents and reproductions. It also applies to the electronic documents described above.

2.5 Record Retention Schedule

The Record Retention Schedule is organised as follows:

Section Topic

A. Accounting and Finance
B. CEIST School Records
C. Personnel Records
D. Correspondence and Internal Memoranda
E. Electronic Documents
F. Electronic Mail (Email)

Classes of Records	Retention Period	Final Disposition (After Retention Period Expires)
ACCOUNTING AND FINANCE		
CEIST Annual Audit Reports	Retain Indefinitely	Archive
Financial Statements	Retain Indefinitely	Archive
CEIST Annual Budget	Retain Indefinitely	Archive
Bank Statements	Hold for current year plus six years	Destroy by confidential shredding
CEIST SCHOOL RECORDS		
School Annual Statistical Data	Retain Indefinitely	Archive
School Annual Reports	Retain Indefinitely	Archive
School BOM Minutes	Retain Indefinitely	Archive
School BOM Correspondence	Retain Indefinitely	Archive
Letters of Appointment	Duration of term	Destroy by confidential shredding
Acceptance forms	Duration of term	Destroy by confidential shredding
BOM Members Contact Details	Duration of term + 6 months	Destroy by confidential shredding
School Finance Sub-Committee (listing of committee members)	Current year plus six years	Destroy by confidential shredding
School Property Data and Correspondence	Retain Indefinitely	Archive
School Policies	Until reviewed	Archive
School Senior Management Appointments Correspondence	18 Months	Destroy by confidential shredding
School Senior Management Appointments Interview Docs	18 Months	Destroy by confidential shredding
School Senior Management Appointments Shortlisting	18 Months	Destroy by confidential shredding
School Senior Management Appointments Interview Applications	18 Months	Destroy by confidential shredding
School Senior Management Appointments Letter to Candidates	18 Months	Destroy by confidential shredding
PERSONNEL RECORDS		
Employee Personnel Records (Including individual attendance records, application forms, job or status change records, performance evaluations, termination papers, training and qualification records).	Current year plus six years after separation	Destroy by confidential shredding
Recruiting Records - All Non-Hired Applicants	Removed post filling of vacancies	Destroy by confidential shredding
Job Descriptions	Current Year plus six years after separation	Destroy by confidential shredding
Pension Calculations	Retain Indefinitely / Lifetime of employee plus seven years	Destroy by confidential shredding

Note: Please consult "Data Protection for Schools" retention policy for any data types which are not listed above.

CORRESPONDENCE AND INTERNAL MEMORANDA

General Principle: Most correspondence and internal memoranda within the CEIST Education Office should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract. It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded *within two years.* Some examples include:

    - Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings.
    - Form letters that require no follow-up.
    - Letters of general inquiry and replies that complete a cycle of correspondence.
    - Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change).
    - Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary.
    - Chronological correspondence files.

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.

ELECTRONIC DOCUMENTS

Electronic documents include Microsoft Office Suite and PDF files. Retention period depends on the subject matter.

PDF documents – The length of time that a PDF file should be retained should be based upon the content of the file and the category under the various sections of this policy.

Text/formatted files - Staff will conduct annual reviews of all text/formatted files (e.g., Microsoft Word documents) and will delete all those they consider unnecessary or outdated.

ELECTRONIC MAIL (Email)

- Staff will strive to keep all but an insignificant minority of their e-mail related to business issues.
- Staff will not store or transfer CEIST related e-mail on non-work-related computers except as necessary or appropriate for company purposes.
- CEIST Staff Electronic email is backed up daily.

E-Mail Retention

CEIST staff emails should be divided into two categories – Routine Emails and Non-Routine Emails.

Routine emails	CEIST **staff routine email to be deleted after 12 months** from staff email accounts. Some examples of routine email include: - Emails that require no acknowledgment or follow-up, such as mails of appreciation, congratulations, and plans for meetings. - Emails of general inquiry and replies that complete a cycle of correspondence. - Emails requesting specific action that have no further value after changes are made or action taken (e.g. name or address change). - Other emails of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary.
Non-Routine emails	Any emails pertaining to non-routine matters or having significant lasting consequences should be marked as important and categorised based on email content. All non-routine emails should then be retained in line with data category in data retention table.

2.6 Data Backups

CEIST does not automatically delete electronic files beyond the dates specified in this Policy. It is the responsibility of all staff to adhere to the guidelines specified in this policy.

Daily an online backup copy of all electronic files saved on CEIST network shares is completed. This online backup completed by external contractor ICT Project Management is a safeguard to retrieve lost information should any files on the network experience problems. The online backup is considered a safeguard for the record retention system of CEIST but is not considered an official repository of CEIST records.

In certain cases, a document will be maintained in both paper and electronic form. In such cases the official document will be the electronic document.

2.7 Data Retention Compliance:

The Data Protection Officer for CEIST will provide up to date guidelines for CEIST Staff and administer IT processes to ensure CEIST adheres to data retention periods set out in this policy and will ultimately be responsible for the deletion of all data within the specified timeframe.

Section 3: CEIST Data Loss Notification Procedure

3.1 Introduction:

The purpose of this document is to provide a concise procedure to be followed in the event that CEIST becomes aware of a loss of personal data. This includes obligations under law, namely the Irish Data Protection Acts 1988 to 2018 and the General Data Protection Act (GDPR) 2018. The procedure is consistent with the guidelines issued by the Irish Data Protection Commissioner in 2010 and enshrined in Irish law.

3.2 Rationale:

The response to any breach of personal data (as defined by the legislation) can have a serious impact on the reputation of CEIST and the extent to which the public perceives CEIST as trustworthy.

The consequential impact on the commercial brand can be immeasurable. Therefore, exceptional care must be taken when responding to data breach incidents. Not all data protection incidents result in data breaches, and not all data breaches require notification. This guide is to assist staff in developing an appropriate response to a data breach based on the specific characteristics of the incident.

3.3 Scope:

The policy covers both personal and sensitive personal data held by CEIST. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by CEIST. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise. This policy should be read in conjunction with the associated Data Protection Policy, Subject Access Request procedure and the Data Retention and Destruction Policy.

3.4 What constitutes a breach, potential or actual?

A breach is a loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users, for an authorised purpose, have access or potential access to personal data in usable form, whether manual or automated.

This could mean:

- Loss of a laptop, memory stick or mobile device that contains personal data
- Lack of a secure password on pc's and applications
- Emailing data that is not disclosed in the public domain to someone in error
- Giving a system login to an unauthorised person
- Failure of a door lock or some other weakness in physical security which compromises personal data

3.5 What happens if a breach occurs?

Actual, suspected, or potential breaches should be reported immediately to the Data Protection Officer (DPO) of CEIST, which is the Information Communications Technology (ICT) Coordinator and also to the Chief Executive Officer (CEO) of CEIST.

Any employee who becomes aware of a likely data breach and fails to notify the CEO or ICT Coordinator will be subject to the disciplinary procedure of CEIST.

A team comprising the DPO, CEO and personnel from the CEIST Board of Directors will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of Data Subjects impacted, the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection.

In certain circumstances CEIST may, (e.g. if required by the Office of the Data Protection Commissioner), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. CEIST will make recommendations to the data subjects which may minimise the risks to them. CEIST will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

3.6 When will the Office of the Data Protection Commissioner be informed?

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner within 72 hours of breach occurring. The only exceptions to this policy are when the data subjects have already been informed, and where the loss involves only non-sensitive, non-financial personal data. Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commissioner is notified only where the data on such devices is not encrypted.

3.7 Data Loss Incident logging.

All data breaches will be recorded in an incident log as required by the Office of the Data Protection Commissioner. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and actions taken. Communication with the Office of the Data Protection Commissioner will also be logged. If the Office of the Data Protection Commissioner was not contacted an explanation of why the Data Commissioner was not informed must also be recorded. Such records will be provided to the Office of the Data Protection Commissioner upon request.

Section 4: CEIST Subject Access Request Procedure

Under the Data Protection Act(s) the key right for the individual is the right of access. Essentially this means that CEIST will be required to supply an individual the personal data that it holds if a valid request is made. Full details are outlined in the CEIST Data Protection Policy. The time limit for complying with an access request is one calendar month from the time which the request has been made. As number of days in a calendar month can vary it is best to aim for full completion within 28 days of request. To ensure compliance with the time limit and other access obligations the following organisational and procedural steps are required:

1) The CEIST ICT Coordinator acts as the CEIST Data Protection Officer and is the person who will be responsible for the response to the access request. A description of the functions and responsibilities of the Data Protection Officer will be circulated within the organisation and staff will be advised of the necessity for co-operation with them.

2) All subject access matters should be submitted to the Data Protection Officer.

3) Check the validity of the access request and ensure that the request was made in writing.

4) No fee will be charged for any Data Access Requests.

5) Check that sufficient material has been supplied to definitively identify the individual. This is most important. This may be the signature, a CEIST Ref ID number in combination with name and address or date of birth. It should not be possible for a third party to provide the material to lodge a false access request.

6) Check that sufficient information to locate the data has been supplied. If it is not clear what kind of data is being requested, more information must be requested from the data subject. This could involve identifying the databases, locations or files to be searched or giving a description of the interactions the individual has had with CEIST.

7) Log the date of receipt of the valid request.

8) Keep note of all steps taken to locate and collate data.

9) If data relating to a third party is involved, do not disclose without the consent of the third party or anonymise such data if this would conceal the identity of the third party. An opinion given by a third party may be disclosed unless it is an opinion which was given in confidence on the clear understanding that it would be treated as confidential.

10) Monitor process of responding to the request – observing time limit of 28 days.

11) Supply the data in an intelligible form (include an explanation of terms if necessary). Also provide description of purposes, disclosee and source of data (unless revealing the source would be contrary to the public interest).

12) Number the documents supplied.

13) Have the response "signed-off" by the CEIST CEO.

14) If an applicant makes a request to be forgotten the Data Protection Officer shall ascertain if the data is required by CEIST for a particular purpose and if it is permitted to do so under the Regulation. If not, the request is complied with and the data erased. If it is permitted to retain the data, the decision to do so is conveyed to the individual with the reasons for retention and a list of data retained.

15) Regular review to be kept of procedures and processes.

Section 5: Policy Review and Approval

This policy will be reviewed in January of every second year following the date of approval or sooner if necessary. Responsibility for initiating the review is with the Information Communications Technology (ICT) Coordinator.

Document History

Approved by Board of CEIST Board	22nd August 2019
To be reviewed	January 2021

Appendix I: Access to Information/Files Request Form

If you are applying for personal data for yourself please complete Sections 1, 3 and 4. If you are applying for personal data on behalf of another person please complete sections 1, 2, 4 and ask the person, for whom you are applying for the data, to fill section 5. All completed forms must be sent by post to CCIST CLG, Summit House, Embassy Office Park, Kill, Co. Kildare, Eir Code: W91 VK0T

1. DETAILS OF THE PERSON REQUESTING THE INFORMATION

Full Name: _____

Address: _____

Telephone Number: _____

Email: _____

Please supply evidence of your identity, i.e., library card, driving licence, birth certificate (or photocopy).

2. If you are you acting **on behalf of another person (third party)**, the written permission of that person must be enclosed.

DETAILS OF THIS PERSON:

Full Name: _____

Address: _____

_____

Telephone Number: _____

Email: _____

Please describe your relationship with this person that leads you to make this request for information on their behalf.

_____

_____

_____

_____

_____

3. If you are applying for records on our own behalf only, list the records or information about yourself that you require to access:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

4. Declaration

I _____, certify that the information given on this application form is true. I understand that it is necessary to confirm my and the other person's (if applicable) identity and it may be necessary to obtain more detailed information in order to locate the correct information.

Signed _____ Date _____

Documents which must accompany this application are:

i) evidence of your identity

ii) evidence of the other person's identity (if different from above) and

iii) evidence of the other person's consent to disclose this information to you.

Please note that we reserve the right to obscure or suppress information that relates to other third parties (under the terms of the Data Protection Acts).

5. **CONSENT FORM TO OBTAIN INFORMATION FOR ANOTHER PERSON (THIRD PARTY) MUST BE SIGNED BY THE THIRD PARTY**

NAME: _____
ADDRESS: _____
_____
_____

I give permission to _____ to access the following records/information on my behalf:

_____
_____
_____
_____

SIGNATURE: _____

DATE: _____

OFFICE USE ONLY
Request received:

_____
_____

Notes:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Date Completed:

_____

Appendix II: CEIST Data Retention and Destruction Policy for Closed Schools

Background

Any school which closes while under the CEIST Trusteeship must pass all data, both hard and soft copies, to CEIST for storage. CEIST then becomes the Data Controller for this school and in turn acts as the school for all Data Protection purposes. This means that all data access requests pertaining to this school must be submitted to CEIST.

Purpose

The purpose of this Policy is to ensure that necessary documents of the school are adequately protected and maintained by CEIST and to ensure that documents and data that are no longer needed by the school and/or of no value are discarded at the proper time and in a secure manner. The basic approach when keeping school records is to always have a purpose for data kept. If there is no purpose for keeping the data, then it should not be kept. The Record Retention Schedule at the end of this document outlines the different types of date which is to be held by the school giving reasons and retention periods for each.

The main enquiries CEIST will receive in relation to closed schools will be proof of staff employment and proof of student attendance. Some examples of good practice when dealing with school records are:

Staff
Personal data relating to school staff such as phone number, bank account, etc. should not be required but proof of staff employment by the school will be needed by staff members in the future for total teaching hours or pension. For these reasons all records of staff employed by the school for each given year should be retained.

Student
Personal data relating to students such as phone number, religious believes, etc. should not be required but proof of student attendance to school may be needed by this student in the future. Therefor all roll book or other forms of registered student lists per school year should be retained.

Policy

This Policy represents CEIST policy regarding the retention and disposal of hard copy documentation and the retention and disposal of electronic documents in relation to a school which has closed down but is under the Trusteeship of CEIST.

Administration

The Record Retention Schedule included towards the end of this document is approved as the initial maintenance, retention and disposal schedule for all physical and computerised records of a closed school under the trusteeship of CEIST. The CEIST ICT Coordinator is the Data Protection Officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed.

Information Sources

The Record Retention Schedule included towards the end of this document is copied from the "Data Protection for Schools" website www.dataprotectionschools.ie. This website is maintained by several school managerial bodies including the Joint Managerial Body for Voluntary Secondary Schools (JMB). This website should be monitored annually for changes and the JMB Data Protection Advisor contacted for any queries regarding retention period issues.

Applicability

This Policy applies to all physical records generated in the course of the school's operation, including both original documents and reproductions. It also applies to the electronic documents described above.

Definitions

Hard Copy Document/Data
Any paper document or document in a printed format.

Soft Copy Document/Data
Any document/data stored on a computerised system.

Document History

Approved by Board of CEIST Board	22nd August 2019
To be reviewed	January 2021

Record Retention Schedule for Closed Schools

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

Records relating to pupils/students	Vol.Sec	Confidential shredding	Comments
Enrolment Forms	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)	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	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	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	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	N/A	Never destroy
Scholarship applications e.g. Gaeltacht, book rental scheme	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**	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	Vol Sec.	Final disposition	Comments
Psychological assessments	Indefinitely	N/A - Never destroy	Never destroy
Special Education Needs' files, reviews, correspondence and Individual Education Plans	Indefinitely	N/A	Never destroy
Accident reports	Indefinitely	N/A	Never destroy

Child protection records	Indefinitely	N/A	Never destroy
Section 29 appeal records	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	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)
Records of complaints made by parents/ guardians	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	**Vol Sec.**	**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.	✓	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.
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)	**Vol. Sec**	**Final Disposition**	**Comments**
e.g. applications, qualifications, references, recruitment, job specification, contract, Teaching Council registration, records of staff training etc.		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)
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		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)
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	✓		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	**Vol Sec.**	**Confidential Shredding**	**Comments**
Sickness absence records/certificates	✓	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	**Vol Sec.**	**Final Disposition**	**Comments**
Records of previous service (incl. correspondence with previous employers)	✓	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	**Vol Sec.**	**Final disposition**	**Comments**
Any returns which identify individual staff/pupils,		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	**Vol Sec.**	**Final disposition**	**Comments**
Board agenda and minutes	✓	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	**Vol Sec.**	**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	✓	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	**Vol Sec.**	**Final disposition**	**Comments**
Audited Accounts	✓	n/a	Indefinitely
Payroll and taxation	✓		Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained **indefinitely** within the school. These records can be kept either on a manual or computer system.
Invoices/back-up records/receipts	✓	✓	Retain for 7 years

Promotion process	Vol Sec.	**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 III: Data Loss Incident Log

Organisation: CCIST	DPO: David Conway

Log Date	Incident Description	Manual/ Automated?	Personal/ Sensitive?	Encrypted?	Volume of Records	DPC Notified?	Notification Date	Additional Reference material