CEIST CLG

Data Protection Policy

Date: _____

CEIST
Catholic Education
An Irish Schools Trust

Table of Contents

Introduction

Purpose of Data Protection

The Data Protection Act 1988 and the Data Protection (Amendment) Act 2003 govern the processing of all personal data. The purpose of the Act is to safeguard the privacy rights of individuals regarding the processing of their personal data by those who control such data. In particular, it provides for the collection and use of data in a responsible way, while providing against unwanted or harmful uses of the data.

Purpose of this document

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 legislation, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).

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, 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.

Background to Irish Law & the Retention of Data

The Data Protection Acts 1988 and 2003 regulate the collection, processing, storage and disclosure of personal information that is processed either electronically or manually. The 2003 Act gave effect to the EU Directive (Directive 95/46/EC) on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.

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. The Act confers rights on any person (including any employee) about whom personal information is kept in a form which can be processed. The Act places duties on those who process or control such data (including employers).

Statement

These guidelines, policy and procedures relate to all files and documents held by CEIST as they relate to personal data on any individual.

CEIST

Any reference to CEIST in this policy is understood to mean CEIST Ltd and their employees.

Personal Data is understood to be:

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 CEIST. It is the understanding of CEIST that it comes within the scope of the Data Protection Act 1988 and 2003. It is also the understanding of CEIST that it does not come within the scope of the Freedom of Information Act.

Sensitive Personal Data means personal data as to -

(a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,

(b) whether the data subject is a member of a trade union

(c) the physical or mental health or condition or sexual life of the data subject,

(d) the commission or alleged commission of any offence by the data subject, or

(e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings;

Policy Statement

CEIST is committed to ensuring that the retention of data by it is carried out, processed and retained in a responsible manner and that the rights of those about whom information is processed and retained is protected.

Principles:

CEIST will administer its responsibilities for the retention of personal data in accordance with the eight data protection principles outlined in the Act as follows:

1. **Obtain and process personal data fairly.**
2. **Keep only for one or more specified and lawful purposes.**
3. **Use and disclose it only in ways compatible with these purposes**
4. **Keep it safe and secure.**
5. **Keep accurate, complete and up-to-date.**
6. **Ensure that it is adequate, relevant and not excessive.**
7. **Retain it for no longer than is necessary for the specified purpose or purposes.**
8. **Give a copy of his/her personal data to an individual, on request.**

Section 1 - Policy, Procedures and Guidelines for the Retention and Protection of Data

1.1 Data Covered by this guideline

Any data as defined above retained by any CEIST personnel in the course of their work.

1.2 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 within schools under CEIST Trusteeship
- 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 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 and Communications Systems Manager** in his capacity as Data Protection Officer is informed, and 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 in the event that 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.

1.3 The Data Protection Principles

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. An employee 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 are 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. As employer we must take care to keep data accurate and up to date because if they are inaccurate or not kept up to date, they may cause damage to the individual concerned who is most likely to be the employee.

CEIST will:

- 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 / purposes, 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.

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.

1.4 Appropriate Security Measures

In determining appropriate security measures the Data Controller:

- may have regard to the state of technological development and the cost of implementing security measures, and
- shall ensure that the security measures provide an appropriate level of security, considering both the nature of the data concerned, and the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss, or damage.

These provisions apply to all Data Controllers, but in particular where the processing involves the transmission of personal data over a network. In this circumstance the data being intercepted by a third party or accidental disclosure to a third party, being lost or corrupted is an obvious risk.

Data Controllers and Data Processors must ensure that their employees / members comply with the above security measures. There should be clear access controls for the transfer of personal data within the organisation's internal computer network. Where personal data is being transmitted over the internet, it should be encrypted.

1.5 Written contract between Data Controller and Data Processor

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 Data Protection legislation.

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.

1.6 Fair processing of personal data

In order to be seen to have processed the data fairly the Data Controller 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.

1.7 Additional conditions for processing personal data

In addition to the eight data protection principles, a Data Controller must not process personal data unless *at least one* of the following conditions is met:

(a) Explicit Consent is given-

The data subject has given explicit consent. Where the data subject by reason of their physical or mental incapacity is or is unlikely to understand the effect of giving consent then another family member can give consent.

(b) For the performance of a contract-

The processing is necessary for the performance of a contract to which the data subject is a party; or in order to take steps at the request of the data subject prior to entering into a contract.

(c) To comply with a legal obligation-

The processing is necessary to comply with a legal obligation.

(d) To protect interests-

To protect the data subject's vital interests, including damage to health or property.

(e) For administration of justice-

The processing is necessary for the administration of justice.

(f) To perform a public function-

The processing is necessary to perform a Government function, or other function of a public nature, or function conferred on an individual under an enactment.

(g) For Legitimate interests-

The processing is necessary for the legitimate interests of the Data Controller or by a third party(ies) to whom the data are disclosed, except where the processing is unwarranted due to prejudicing the rights, freedoms and legitimate interests of the data subject.

1.8 Processing of sensitive data

In addition to the other provisions governing the processing of personal data, the Data Controller, under the Act, in order ***to process sensitive data*** must meet at *least one* of the following conditions:

1. The data subject has given explicit consent. Where the data subject by reason of their physical or mental incapacity is or is unlikely to understand the effect of giving consent then another family member can give consent.

2. The processing is necessary for the Data Controller to comply with legal obligations connected with employment.

3. To protect the data subject's vital interests, including damage to health or property, where it is not possible to obtain consent, or where another persons health or property could be damaged where such consent is unreasonably withheld.

4. The processing is carried out by a non-profit organisation, that exists for political, philosophical, religious or trade union purposes, as part of its legitimate activities. The processing is carried out with appropriate safeguards for the rights and freedoms of data

subjects, and relates only to members of the body or to individuals who have regular contact with the body in connection with its purposes. The processing does not involve disclosure to a third party without the data subject's consent.

5. The data subject has made the information public.
6. The processing is necessary to perform a Government function, or function conferred on an individual under an enactment.
7. The processing is necessary to obtain legal advice, or connected with legal proceedings, or for defending legal rights.
8. The processing is needed for medical purposes undertaken by a health professional, or by another individual who would owe the data subject a similar duty of confidence as a health professional.
9. The processing is necessary to obtain information for statistical purposes, in accordance with the Statistics Act, 1993.
10. The processing is carried out by political parties, candidates for election, or holders of elective office, in the course of electoral activities for compiling data on people's political opinions.
11. The processing is authorised by Ministerial regulation.
12. The data subject has provided data for the assessment or payment of any tax or duty owed.
13. The processing is necessary for determining entitlement to or control of state benefits.

1.9 Duty of care

The Data Controller and Data Processor must exercise a duty of care towards data subjects.

1.10 Rights of Data Subjects

- The data subject has a right to establish the existence of personal data.
- The data subject may submit a written request to ascertain if the organisation, its members or employees keeps personal data related to them.
- The Data Controller must respond within 21 days as to whether such data are kept and, in the event they are, with a description of the data and the purposes for which they are kept.

1.11 Right of access

The individual is entitled, on foot of a written request, to be:

- informed by the Data Controller 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 the Data Controller has as to the source of the data; and
- (where the processing of the personal data is by automatic means, and this forms the sole basis for any decisions affecting the data subject) to be informed by the Data Controller of the logic involved in the processing. This provision does not apply where it would adversely affect trade secrets or intellectual property, in particular any copyright protecting computer software.

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. ***The Data Controller has 40 days within which to comply with such a request.***

1.12 Access Fee

CEIST will not charge any fee for data access requests.

1.13 Subsequent Requests

If a Data Controller has previously complied with a request, he/she 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.

1.14 Proof of Identity

The individual making the access request must provide the Data Controller with:

- proof of identity, and
- reasonable information to locate any relevant personal data.

The Data Controller is not obliged to disclose to a data subject personal data relating to another individual, without his/her consent.

1.15 Refusal to comply with a request

A refusal 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.

1.16 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.

1.17 Restriction of right of access

The entitlement to access personal data **does not apply** to the following:

(a) personal data kept for the purpose of preventing, and/or investigating offences, or collecting taxes or other monies payable to state bodies, where access to the data would prejudice any of the above matters;

(b) where the personal data mentioned above is kept for discharging a legal obligation;

(c) any situation where access to the personal data would be likely to prejudice the security of a prison.

(d) where the personal data are legally required to protect members of the public against financial loss due to incompetence or malpractice;

(e) where accessing the personal data would be contrary to protecting the international relations of the state;

(f) where the personal data are kept for the purpose of estimating the amount of the liability of the Data Controller on foot of a claim for damages and where granting the access

request would prejudice the Data Controller s interests;

(g) where a claim of legal privilege could be maintained regarding the personal data in communications between a client and his/her professional advisers;

(h) information kept by the Commissioner or the Information Commissioner for the purposes of his or her functions;

(i) the personal data are kept only for the purpose of carrying out research and the statistics are not made available in a form that identifies the data subjects;

(j) back-up personal data.

1.18 Right of rectification or erasure

The Data Controller must comply with a written request to have personal data rectified, blocked or erased, if he/she has contravened any of the provisions for collecting, processing, use and disclosure of the data. The Data Controller must respond within 40 days to the request and notify the individual and also, if the data has been significantly modified, any person to whom the data were disclosed during the previous 12 months.

1.19 Right to object to data processing likely to cause damage or distress

An individual is entitled, in writing, to request the Data Controller, in a reasonable time, to stop processing, or not to begin processing, any personal data of which he/she is the data subject.

This applies if the processing is:

- for the performance of a task carried out in the public interest;
- in the exercise of official authority vested in the Data Controller or a third party to whom the data are to be disclosed,
- necessary for the legitimate interests of the Data Controller, unless those interests are overridden by the interests of the data subject, and
- likely to cause substantial damage or distress to the data subject, or another person, and
- the damage or distress is unwarranted.

The Data Controller must respond within 20 days to the individual stating that the request has been complied with, or giving the opinion that the request is unjustified along with the reasons for the opinion.

If a Data Controller refuses to comply with a request to cease processing, and the individual makes application to the Data Protection Commissioner, the Commissioner may serve an enforcement notice on the Data Controller, ordering that steps are taken to comply with the request, and the Commissioner's reasons for making such an order. The Commissioner will allow 40 days to elapse before the enforcement notice is issued.

This right to object to processing does not apply if:

- the data subject has given his/her explicit consent;
- if the processing is necessary for the performance of a contract, to which the data subject is a party;
- in order to take steps at the request of the data subject, prior to entering into a contract;
- for the Data Controller to comply with legal obligations;
- to protect the vital interests of the data subject;
- it is carried out by political parties, or candidates for election, or holders of elective office in the course of electoral activities;
- the circumstances are covered by Ministerial regulation.

1.20 Rights in relation to automated decision making

(e.g. decisions based on automated data)

Decisions which have legal effect, or affect the data subject in some other significant way, **may not be based solely** on personal data being processed by automatic means. The types of personal matters that this right relates to includes, the data subject's performance at work, creditworthiness, reliability or conduct. *(This is not an exhaustive list).* This does not apply where the decision:

- is made for the purpose of considering whether to enter into a contract with the data subject, or with a view to entering such a contract, or in the course of performing such a contract;
- is authorised or required by law, and the data subject has been informed of the proposal to make the decision, which will either grant a request of the data subject, or adequate steps have been taken to safeguard the legitimate interests of the data subject by, for example, making arrangements to enable him/her to make representations to the Data Controller in relation to the proposal, or
- if the data subject consents to the automatic processing.

1.21 Right to object to direct marketing

Where personal data are kept for direct marketing purposes the data subject can request the Data Controller in writing:

- not to process the data for that purpose, or
- to stop processing the data for that purpose.

If the request is not to process the data for that purpose the Data Controller must:

- erase the data if they are only used for that purpose, or
- if they are used for other purposes, only use them for those other purposes in future.

The Data Controller must comply with the request within 40 days and to notify the data subject accordingly. If the data is processed for other purposes the data subject must be informed of those other purposes. Where a Data Controller believes that personal data in his/her possession may be used for direct marketing purposes, he/she must inform the data subjects that they have a right to object, in writing, free of charge to such processing.

1.22 Where restrictions on the disclosure of personal data do not apply

The restrictions on the disclosure of personal data do not apply if the disclosure is required to:

(a) safeguard the security of the State;

(b) prevent, and investigate offences, or collect any tax or monies owed to the State;

(c) protect the international relations of the State;

(d) prevent injury or damage to property;

(e) meet legal requirements;

(f) obtain legal advice, or for the purpose of legal proceedings;

(g) meet a request from, or with the consent of, the data subject, or a person acting on his/her behalf.

1.23 Exemptions under the Act

The Act does not apply where personal data:

- are or were kept for State security measures;
- consist of information that is required to be made available to the public by law, however, if this personal data is used for another purpose the exemption will no longer apply to it;
- are kept by an individual for the management of his/her personal affairs;

1.24 Historical research

The provisions regarding the collection, processing, keeping, use and disclosure of personal data, the additional provisions regarding processing data, and sensitive data, will not apply if the data are kept solely for the purpose of historical research, and the keeping of which complies with any requirements prescribed for safeguarding the rights and freedoms of data subjects.

1.25 Liability

If the organisation is found guilty of an offence under the Data Protection Act, it will be liable:

- up to €10 million or 2% of total worldwide annual turnover (whichever is greater) for serious breaches; and
- up to €20 million or 4% of total worldwide annual turnover (whichever is greater) for very serious breaches.

In addition data subjects will have a right to sue for non-material damage in addition to material damage arising from data privacy breaches.

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

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.

1. DETAILS OF THE PERSON REQUESTING THE INFORMATION

Full Name: _____

Address: _____

_____

Telephone Number: _____ Fax: _____

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: _____ Fax: _____

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: _____