Scoil Phobail Chabán tSíle
Cabinteely Community School

Data Protection Policy

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Cabinteely Community School. 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

Cabinteely Community School 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 Cabinteely Community School in relation to its staff, service providers and clients in the course of its activities. Cabinteely Community School makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by Cabinteely Community School. 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 Cabinteely Community School. 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, the Data Retention and Destruction Policy, the Data Retention Periods List and the Data Loss Notification procedure.

Cabinteely Community School as a Data Controller

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

- Employees of Cabinteely Community School
- Customers of Cabinteely Community School
- Third party service providers engaged by Cabinteely Community School
- (*expand list as appropriate*)

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, Cabinteely Community School is committed to ensuring that their staffs 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 Data Protection Officer is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by Cabinteely Community School, there is regular and active exchange of personal data between the school and its Data Subjects. In addition, Cabinteely Community School exchanges personal data with Data Processors on the Data Subjects' behalf.

This is consistent with Cabinteely Community School's obligations 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 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.

Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed as soon as possible.

It is intended that by complying with these guidelines, Cabinteely Community School will adhere to best practice regarding the applicable Data Protection legislation.

Third-Party processors

In the course of its role as Data Controller, Cabinteely Community School 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.

These Data Processors include:

- (*list as appropriate*)

The Data Protection Principles

The following key principles are enshrined in the Irish legislation and are fundamental to the Cabinteely Community School's Data Protection policy.

In its capacity as Data Controller, Cabinteely Community School ensures that all data shall:

1. ... be obtained and processed fairly and lawfully.

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller (Cabinteely Community School)
- 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.

Cabinteely Community School 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, Cabinteely Community School will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, educational and contractual necessity, etc.;
- Where Cabinteely Community School 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 Cabinteely Community School's lawful activities, and Cabinteely Community School 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 Cabinteely Community School and operating on its behalf.

2. .... be obtained only for one or more specified, legitimate purposes.

Cabinteely Community School 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 Cabinteely Community School holds their data, and Cabinteely Community School 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 Cabinteely Community School will be compatible with the purposes for which the data was acquired.

4. .... be kept safe and secure.

Cabinteely Community School 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 Cabinteely Community School in its capacity as Data Controller.

Access to and management of staff and customer records is limited to those staff members who have appropriate authorisation and password access.

5. ... be kept accurate, complete and up-to-date where necessary.

Cabinteely Community School 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. Cabinteely Community School 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.

Cabinteely Community School 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).*

Cabinteely Community School has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the respective retention period has elapsed, Cabinteely Community School undertakes to destroy, erase or otherwise put this data beyond use.

8. *... be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.*

Cabinteely Community School 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.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, Cabinteely Community School's staff engages 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 Cabinteely Community School, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which Cabinteely Community School must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

Cabinteely Community School's staff will ensure that, where necessary, such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 days from receipt of the request.

Implementation

As a Data Controller, Cabinteely Community School 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 Cabinteely Community School's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of Cabinteely Community School's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Caretakers

- Security of school buildings, locking gates, locking doors etc.
- Ensure alarms are switched on and working.
- Ensure that CCTV systems are working and are maintained/serviced appropriately.
- Ensure that only authorised persons have access to school buildings.
- Storage of confidential wastepaper until it is securely shredded.
- Report any personal date breaches immediately to the principal.
- Comply with and give assistance during audits, spot-checks and inspections.

Clerical staff/Receptionist/School Secretary

In addition to all those items listed above,

- Keep the reception area clean and tidy.
- Ensure that personal data is not visible to others (e.g. leaving files on desk).
- Keep personal data out of sight of visitors to reception area.
- Ensure that their computer screen is not visible to visitors at reception.
- Diligence and attention to detail when entering data on to the school administrative system.
- Keep the data accurate, complete and up to date.
- Adhere to information governance protocols if making changes (deletions, additions etc).
- Identify data subject requests when they are received (by letter, email etc). If received by telephone, asking the person to put their request in writing. Ensure that all such requests (whether by phone, in person or by email or in writing) are immediately escalated to the Principal without delay.
- Being cautious about requests for information, where a request for personal data is received, asking the requester to verify their identity, ascertaining whether the requester is legally entitled to obtain the personal data. E.G. request for personal data relating to a student from a journalist, request to access list of students by a politician, request for CCTV footage from a solicitor etc. Asking the requester to put their request in writing. Escalating requests to the Principal without delay.
- Being suspicious, alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.
- Prepare post with high levels of diligence and attention to detail. Ensuring that the correct letter is put in the correct envelope. Developing post protocol checklist (e.g. double checking enclosures, envelope counts etc).
- Prepare emails with high levels of diligence and attention to detail,
  - Ensuring that the correct email address is entered.
  - Using “bcc” instead of to field where appropriate.
  - Encrypting emails where appropriate.
  - If emailing to a group, verifying who the members of the group are.
- Be cautious and suspicious if an email asks you to click on links or open an attached document (even if from a familiar sender rom a genuine email address).
- Keep anti-virus and anti-malware software p to date, install patches when required.
- Ensure that data are keep safe and secure.
- Use strong passwords (12 characters, mixture of alphanumeric, upper and lower case and symbols e.g. %, £, & etc) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students).
- Ensure passwords are unique (e.g. do not use the same password for your PayPal account as for your VSWare account etc).
- Respect access-permission levels, never snooping into files/records to which you have no genuine employment reason for accessing, adhering to the principle of “need to know”.
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data.
- Adhere to all school policies and protocols.
- Follow all instructions given by the Principal.

Teaching Staff, SNA's, etc

In addition to all those listed above

- Adherence to high standards of ethics and professionalism in all data entries (e.g. when entering notes about a student on the VSware system). Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data.
- Ensure that any handwritten notes in any notebook are transferred to the school administrative system as soon as possible (to ensure availability of data, allowing appropriate back-ups to be made, accountability, transparency, keeping data safe and secure, etc).
- Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts etc).
- Never sharing work-related data on unapproved systems (e.g. talking about a student in a teachers WhatsApp group).
- Assisting the Principal with access requests.
- Giving constructive feedback around how policies and protocols can be improved.

Key Players (Guidance Counsellor, School Nurse, etc).

In addition to all those listed at (1) – (3) above, school personnel with additional responsibilities and access to particularly sensitive data must:

- Adhere to ethical standards required by their professional/representive bodies (Institute of Guidance Counsellors, Nursing and Midwifery Board of Ireland etc) around confidentiality, record keeping, etc.
- Have a clear understanding of when and in what circumstances data should be shared (e.g. child protection, child welfare, medical needs, etc).
- Take responsibility for keeping their sensitive data-sets safe and secure (encryption, pseudonymisation etc).
- Exercising good judgment and professionalism in note-taking.

Principal, Deputy Principal, Year Heads etc.

In addition to all those listed at (1) – (4) above:

- Developing policies, procedures, and protocols.
- Driving privacy and data protection awareness.
- Identifying training needs and arranging for refresher training sessions.
- Escalating appropriate issues to the Board of Management.
- Taking appropriate preventive actions to mitigate the risk of data breaches arising.
- Spearheading the response to any data breach (following the data breach protocol).
- Due diligence of service providers (data processors) prior to any service provider being retained.
- Ensuring adequate assurances of GDPR compliance are obtained ("controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject").
- Ensuring appropriate written contracts in place with all service providers.
- Periodic reviews of all arrangements with service providers.

- Record-keeping (Article 30) ("maintain a record of processing activities under its responsibility").
- Undertaking Data Protection Impact Assessments in appropriate circumstances.
- Overseeing data subject right requests (Article 15 – access, Article 16 – rectification, Article 17 – erasure etc, etc).
- Performance management and/or disciplinary process for staff who are not following policies and procedures.
- Working closely with the DPO (see (6) below).
- Seeking advice from management body and/or School's legal advisors where appropriate.
- Keeping up to date with legal developments, sectoral guidance etc.
- Attending in-service training sessions arranged by management body.

Board of Management

In addition to monitoring adherence to (1) – (5) the above:

- Appointing DPO (see Article 37 GDPR for those bodies that are required to appoint a DPO. Current definition of "public authority" in Irish Data Protection Bill could include a School).
- Supporting the Principal and senior management team.
- Review the implementation, effectiveness, and compliance with policies, procedures, protocols.
- Data protection issues as an agenda item at Board of Management meetings.

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, Cabinteely Community School 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 Cabinteely Community School 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.