Data Protection and Record-keeping Policy

Introduction

Our Data Protection policy has been upgraded to incorporate GDPR regulations which are in effect across the EU from Friday 25th May 2018. From that day all businesses/institutions have to follow guidelines that explicitly state a number of requirements for those who obtain personal data of people. For us as a staff that means a number of changes that will have to take place and being aware of the main aspects of Data Protection.

According to the EU now

a) Everyone has the right to the protection of personal data concerning him or her.
b) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data relating to him and her and the right to have it rectified.

There are 8 rules of Data Protection:

- Obtain and process information fairly
- Keep it for one or more specified, explicit and lawful purposes
- Process it only in ways compatible with the purpose for which it was given initially
- Use and disclose it in ways compatible with these purposes
- Keep it safe and secure
- Ensure it is adequate and not excessive
- Retain no longer than necessary
- A copy of the data must be made available to the data subject on request.

Rationale

A policy on data protection and record keeping is necessary to fulfil the requirements as outlined in

- GDPR EU Regulations 2018
- Data Protections Acts 1988 and 2003
- Education Act - Section 9g [requiring a school to provide access to records to students over 18/parents]
- Education Welfare Act – Section 20 [requiring a school to report school attendance and transfer of pupils]
- Section 28 of the Education Welfare Act 2000 which specifies that the data controller may supply personal data kept by him/her to the data controller of another prescribed, provided s/he is satisfied that it will be used for a “relevant purpose” only.

- A policy is necessary to ensure that the school has proper procedures in place in relation to accountability, transparency and storage.
- Good practice to record pupil progress so as to identify learning needs and action to address these needs.
- Fulfil requirements for filling in Primary Online Database as required by Department of Education

Relationship to School Ethos
We promote openness and co-operation between staff, parents and pupils as a means of providing a supportive environment where students can develop to their full potential.

Aims/Objectives
- To ensure the school complies with legislative requirements.
- To ensure that the data protection rights of students, staff and other members of the school community are safeguarded.
- To clarify the types of records maintained and the procedures relating to making them available to the relevant bodies.
- To put in place a proper recording and reporting framework on the educational progress of pupils.
- To establish clear guidelines on making these records available to parents and past pupils who are over 18.
- To stipulate the length of time records and reports will be retained.

Why we collect data
- To support learning
- To monitor progress
- To Provide pastoral care
- To be able to make health care or educational referrals
- To comply with the law
- To safeguard pupils

Guidelines
The Principal assumes the function of data controller and supervises the application of the Data Protection Act within the school. The data under the control of the Principal comes under the following headings.

1. **Personal Data**
This data relates to personal details of the students such as name, address, date of birth, gender, ethnic origin, nationality, religious belief, medical details, dietary information, PPSN, contact details and parents' names. This information is kept in a locked filing cabinet in the office. This information is gathered with the consent of parents for the Department of Education, for the National School Census and Primary Online Database.

2. **Student Records**
Paper records are stored in a filing cabinet in the Principal's office and a locked cupboard in the Special Education Room.

Student records may contain:

- Personal details of the student including PPS number, details of parents names, addresses, contact numbers, religious beliefs, membership of a minority group where relevant. A full outline of all of the data requested for Primary Online Database [POD] along with how this data will be used, accessed and shared is given in the POD Fair Processing Notice available on the "POD" area of the Department's website on www.education.ie.
- Medical data and doctor details.
- School report cards.
- Psychological/Clinical/Occupational Therapy/Speech and Language Assessments.
- Standardised Test Results.
- Attendance Records.
- Assessment tests /Screening Test
- Records of students who have been granted exemption for the study of Irish.
- Teacher – designed tests. Each class teacher designs his/her own test template.
- Individual Education Plans and records of meetings with the stake holders regarding these plans.
- Learning Support/Resource Data such as records of permission/refusal to access LS/RT services in the school.
- Portfolios of student work e.g. Art, Projects.
- Details of behavioural incidents/ bullying incidents or accidents.

3. **Staff Data**
This data relates to personal and professional details of staff such as name, address, date of birth, contact details, payroll number, attendance records, qualifications, school records, sick leave, CPD, curriculum vitae, school returns, Garda Vetting certificates, conduct records.

4. **Administrative Data**

- Enrolment applications and copy of birth certificates.
- Accident Report Book detailing injury and treatment applied.
- Administration of Medicines Indemnity Form.
- Record of books rented under book rental scheme.
- Pupil behaviour records and records of allegations and incidents of bullying and alleged bullying.
- Records in line with Children First Procedures.
- Board of Management files including minutes of meetings and names, addresses and contact numbers of members.
- School accounts.
- Records kept for administrative purposes.

Access to Records

- The following will have access to the data listed above where relevant and appropriate:
- Parents/guardians. Past pupils over 18.
- Health Service Executive staff.
- National Educational Psychological Service.
- National Education Welfare Board.
- Designated school personnel.
- Department of Education & Skills.
- Inspectorate.
- First and second-level schools (once it has been confirmed by the receiving school that the child has been enrolled).
- Board of Management of Cabra Central National School.

With the exception of child protection-related data which is governed by Children First Guidelines and Procedures 2017, data on attendance [NEWB/ TUSLA] and data regarding achievements in literacy and numeracy (National Strategy for literacy and numeracy), a parental authorisation form must be completed by parents in the event of data being transferred to outside agencies. Outside agencies requesting access to records must do so in writing or by phone. Parents/Guardians can make such a request either by phone, email or in writing. Past pupils and parents of past pupils seeking data must do so in writing.

The Annual School Report format in accordance with NCCA guidelines are sent to parents in June. Reports are sent home with pupils following a text-a -parent message. The results of standardised testing of pupils are kept in a folder and stored in a locked filing cabinet in the office. See our Assessment and Recording Policy.

Data Storage

- Location: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Employees are required to maintain the confidentiality of any data to which they have access.
- Security: Paper Records are kept in a secure filing cabinet in the office. Computer records are kept on password protected PCs.
- Computer systems are password restricted.
- Personal information on computer screens and in files is shut down and put away as soon as possible after use.
- Personal data no longer required is shredded.
- Old computers have their memory wiped before they are disposed of.
- Teachers must use school laptops solely for school business and are responsible for ensuring that they are not used or viewed by any other party.

Data Accuracy

Data held will be accurate and as up to date as is reasonably possible. When a pupil informs the school of a change of circumstances their record is updated as soon as is practicable. If a pupil should inform the school that personal data is inaccurate then the school will seek to remedy this is quickly as possible.

Length of time for Storage

Personal data will not be consciously kept for longer that is necessary to fulfil the function for which it was first recorded. Our school will follow the guidelines on the schedule of record retention attached. All records are stored in the school until the past pupil reaches the age of 21 + 7 Years.

Examination results

(a) Categories: The school will hold data comprising examination results in respect of its students. These include class, mid-term, annual, continuous assessment and standardised test results.

(b) Purposes: The main purpose for which these examination results and other records are held is to monitor a student's progress and to provide a sound basis for advising them and their parents or guardians about their education. The data may also be aggregated for statistical/reporting purposes, such as to compile results tables. The data may be transferred to the Department of Education and Skills, the National Council for Curriculum and Assessment and such other similar bodies.

Standardised tests booklets are shredded but the results are kept on record indefinitely.

Roll books are kept indefinitely.

Links to other policies and to curriculum delivery

Our school policies need to be consistent with one another, within the framework of the overall School Plan. Relevant school policies already in place or being developed or reviewed, shall be examined with reference to the data protection policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

Child Protection Statement
Anti-Bullying Policy
Code of Behaviour
Admissions/Enrolment Policy
CCTV Policy
Substance Use Policy
ICT SPHE

Processing in line with data subject's rights

Data in this school will be processed in line with the data subjects' rights.

Data subjects have a right to:

(a) Request access to any data held about them by a data controller
(b) Prevent the processing of their data for direct-marketing purposes
(c) Ask to have inaccurate data amended
(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

Dealing with a data access requests

Under Article 13 and 14 of the GDPR, you have a right to be informed as to how your personal data is being processed. Under Article 15 of the GDPR, you have a right to obtain a copy, of any information relating to you kept on computer or in a structured manual filing system or intended for such a system by any organisation. All you need to do is put your request in writing to the Board of Management
You may be asked to provide evidence of your identity. This is to make sure that personal information is not given to the wrong person.

Our school will be obliged to respond to your access request within one month of receiving the request. In certain limited circumstances, the one month period may be extended by two months (taking into account the complexity of the request and the number of requests). Where our school is extending the period for replying to your request, it must inform you of any extension, and the reason(s) for the delay in responding, within one month of receiving the request.
There is no fee payable by you to make an access request - the organisation must deal with your request for free. However, where the organisation believes a request is manifestly unfounded or excessive (for example where an individual makes repeated unnecessary access requests), the organisation may either charge a fee taking into account its administrative costs in dealing with the request(s), or refuse to act on the request(s). The burden of demonstrating why a request is manifestly unfounded or excessive rests on the organisation.

Exceptions to the right of access

The Data Protection Act 2018 sets out some limited circumstances in which an organisation may not be required to provide you with a copy of your personal data. In particular, an organisation may be exempt from providing you with personal data if a restriction of your right of access is necessary:

- to safeguard cabinet confidentiality, judicial independence and court proceedings, parliamentary privilege, national security, defence and the international relations of the State
- for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties
- in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure
- in respect of damages, compensation or other liabilities or debts related to the claim, or

- For the purposes of estimating the amount of the liability of an organisation on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the interests of the organisation in relation to the claim.

In addition, an organisation may not be required to provide you with a copy of your personal data where the data consists of an expression of opinion about you by another person given in confidence, or on the understanding that it would be treated as confidential, to a person who has a legitimate interest in receiving the information. GDPR also provides that the right to obtain a copy of your personal data must not adversely affect the rights and freedoms of others. For example, when responding to an access request, an organisation should not provide the requestor with personal data relating to a third party that would reveal the third party's identity.

.

Providing information over the phone

- In our school, any employee dealing with telephone enquiries should be careful about disclosing any personal information held by the school over the phone. In particular the employee should:
- Check the identity of the caller to ensure that information is only given to a person who is entitled to that information.
- Suggest that the caller put their request in writing if the employee is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified.
- Refer the request to the principal for assistance in difficult situations. No employee should feel forced into disclosing personal information.
- Implementation arrangements, roles and responsibilities
- In our school the board of management is the data controller and the principal will be assigned the role of co-ordinating implementation of this Data Protection Policy and for ensuring that staff who handle or have access to *Personal Data* are familiar with their data protection responsibilities.

The following personnel have responsibility for implementing the Data Protection Policy:

Name	**Responsibility**
Board of management:	Data Controller
Principal:	Implementation of Policy
Teaching personnel:	Awareness of responsibilities
Administrative personnel:	Security, confidentiality
IT personnel:	Security, encryption, confidentiality