

*Gaelscoil Bhrian Bóroimhe,
Coill na nÚll,
Sord,
Co. Átha Cliath*



Scoil Idirchreidmheach

Fón: 8902799

Faics: 8700044

U.R. 20095C

Suíomh Idirlín: www.gsbb.ie

Ríomhphost: oifig@gsbb.ie

Data Protection Policy 2019

Introductory Statement

The school's data protection policy sets out, in writing, the manner in which personal data on staff, students and other individuals (e.g. parents, members of board of management etc.) are kept and how the data concerned is protected.

This policy was formulated by the school staff in conjunction with the Board of Management in November 2019.

Scope

The policy applies to the keeping and processing of personal data, both in manual form and on computer, including personal data held on both school staff and students.

Data: means information in a form which can be processed. It includes automated data (information on computer or information recorded with the intention of putting it on computer) and manual data (information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system).

Relevant filing system: means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible.

Personal data: means data relating to a living individual who is or can be identified from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Data Controller: A data controller is the individual or legal entity which controls the contents and use of personal data. The school can be considered to be the data controller, with the principal acting for the board of management in exercising the functions involved.

The policy applies to all school staff, the board of management, parents/guardians, students and others insofar as the measures under the policy relate to them.

Rationale

- Schools are obliged to comply with the Data Protection Act, 1988 and the Data Protection (Amendment) Act, 2003 (henceforth referred to as the Data Protection Acts)

- Under Section 9(g) of the Education Act, 1998, the parents of a student, or a student who has reached the age of 18 years, must be given access to records kept by the school relating to the progress of the student in his or her education.
- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the school.
- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day.
- Under Section 28 of the Education (Welfare) Act, 2000, the data controller may supply personal data kept by him or her, or information extracted from such data, to the data controller of another prescribed body if he or she is satisfied that it will be used for a “relevant purpose” only. See Section B.3 under Key Measures below.

Relationship to characteristic spirit of the school (school’s mission/vision/aims)

Gaelscoil Bhrian Bóirimhe endeavors to enable every student to develop their potential in a safe and enjoyable learning environment.

Goals/Objectives

1. To ensure that the school complies with the Data Protection Acts.
2. To ensure compliance by the school with the eight rules of data protection as set down by the Data Protection Commissioner based on the Acts (see below).
3. To ensure that the data protection rights of students, staff and other members of the school community are safeguarded.

Key measures (content of policy)

A. Details of all personal data which will be held, the format in which it will be held and the purpose(s) for collecting the data in each case: (MR=Manual Record, CR=Computer Record, MCR=Manual & Computer Record)

The personal data records held by the school may include:

Staff records: These may include:

- Name, address and contact details, PPS number: MCR- Communication & Contact
- Original records of application and appointment: MCR – Comply with DES & Teaching Council guidelines
- Record of appointments to promotion posts: MCR – Comply with DES guidelines
- Details of approved absences (career breaks, parental leave, study leave etc.) MCR – Record of duration and number of absences.
- Details of work record (qualifications, classes taught, subjects etc) MCR – Staff profile and class distribution
- Details of complaints and/or grievances including consultations or competency discussions, action/improvement/evaluation plans and record of progress. MCR - Record

Student records: These may include:

- Information which may be sought and recorded at enrolment, including:

- name, address and contact details, PPS number: MCR – communication, DES
- names and addresses of parents/guardians and their contact details : MCR – communication
- religious belief: MCR – DES & teaching of religion
- racial, ethnic or national origin: MCR – DES and POD
- membership of the Traveller community, where relevant: MCR – DES & POD
- any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply :MCR – Care of student & DES
- Information on previous academic record: MCR – Education of child
- Psychological assessments: MCR – Education of child
- Attendance Records: MCR – Welfare of child
- Academic record – subjects studied, class assignments, examination results as recorded on official school reports: MCR – Education of Child & DES
- Records of significant achievements: MCR: Progression of Child
- Records of disciplinary issues and/or sanctions imposed: MCR – comply with legislation
- Other records e.g. records of any serious injuries/accidents etc.: MCR – comply with legislation

Board of Management records: These may include:

- Name, address and contact details of each member of the board of management: MCR - Communication
- Records in relation to appointments to the board: MCR – School Patron
- Minutes of board of management meetings and correspondence to the board which may include references to particular individuals: MCR – Recording of decisions taken.

B. Details of arrangements in place to ensure compliance with the eight rules of data protection

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it 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 purpose or purposes
8. Give a copy of his/her personal data to that individual on request.

1. Obtain and process information fairly:

- Form sent to parents, members of staff and members of the Board of Management to be signed stating that they are aware of the data that is kept and rationale for same.
- Personal information is processed fairly in accordance with the Data Protection Acts, with consent being obtained from staff members, parents/guardians or students, where required.
- Sensitive personal information is processed fairly in accordance with the Data Protection Acts, with explicit consent being obtained from staff members, parents/guardians or students, where required.

2. Keep it only for one or more specified, explicit and lawful purposes:

- Persons whose data is collected know the reason/s why it is collected and kept.
- The purpose for which the data is collected and kept a lawful one.
- School management is aware of the different sets of data which are kept and the specific purpose of each.

3. Use and disclose it only in ways compatible with these purposes:

- Data is used only in ways consistent with the purpose/s for which it was obtained.
- Data is disclosed only in ways consistent with that purpose.
- There is a procedure in place, which is in accordance with the Data Protection Acts to facilitate the transfer of information to another school when a student transfers. Permission is sought from parents in advance of transfer of information.

Note: Under Section 20 of the Education (Welfare) Act, 2000, each school principal must maintain a register with the names of all children attending that school. When a child is transferring from the school, the principal must notify the principal of the new school of any problems relating to school attendance that the child concerned had and of any other matters relating to the child's educational progress that he or she considers appropriate. Under Section 28 of the Act, schools may supply personal data, or information extracted from such data, to other schools or another prescribed body if they are satisfied that it will be used in recording the student's educational history, monitoring the student's educational progress or developing the student's full educational potential. The bodies which have been prescribed (and so can share information) under Section 28 are:

- The Minister for Education and Science (which includes the Inspectorate and the National Educational Psychological Service (NEPS))
- The National Council for Special Education (NCSE)
- The National Educational Welfare Board (NEWB)
- Each school recognised in accordance with section 10 of the Education Act, 1998
- Each place designated by the Minister under section 10 of the Education Act, 1998 to be a centre for education.
- The circumstances in which personal data may be disclosed to third parties, including the Department of Education and Science, the NEWB, Gardaí, in legal proceedings, HSE personnel etc are child protection, by parental request or legal requirement.
- The procedure in place, which is in accordance with the Data Protection Acts to facilitate the transfer of personal data abroad is use of registered post or e-mail with password requirement.

Exceptions to disclosure rule:

- Data can be disclosed when required by law
- Data can generally be disclosed to an individual himself/herself or with his/her consent (see 8 below).

4. Keep it safe and secure:

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

- Access to the information (including authority to add/amend/delete records) is restricted to authorised staff on a "need to know" basis?
- Information is made available to the Principal, Deputy Principal, Assistant Principal 1 and to teachers working directly with the child, based on this "need to know" policy?
- Computer systems are password protected.
- Information on computer screens and manual files is kept out of view of callers to the school/office.
- Back-up procedures in operation for computer held data.
- All reasonable measures are taken to ensure that staff are made aware of the security measures, and comply with them.
- All waste papers, printouts etc. are disposed of carefully.

- Steps are taken to ensure that no unauthorised person can access data from computers which are no longer in use or subject to change of use.
- The Principal and Deputy Principal are designated persons responsible for security.
- There are periodic reviews of the measures and practices in place.
- Premises are secure when unoccupied.
- There is a contract in place with a data processor which imposes an equivalent security obligation on the data processor.

5. *Keep it accurate, complete and up-to-date:*

- Clerical and computer procedures are adequate to ensure high levels of data accuracy.
- Appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.

6. *Ensure that it is adequate, relevant and not excessive:*

- The information held is adequate in relation to the purpose/s for which it is kept.
- The information held is relevant in relation to the purpose/s for which it is kept.
- The information held is not excessive in relation to the purpose/s for which it is kept.

7. *Retain it for no longer than is necessary for the purpose or purposes:*

In general, personal data should not be kept for any longer than is necessary to fulfil the function for which it was first recorded. Retention times cannot be rigidly prescribed to cover every possible situation and schools need to exercise their individual judgement in this regard in relation to each category of records held. However, the following particular requirements should be met:

- School registers and roll books are required to be kept indefinitely within the school. Consideration is being given to amending the Data Protection Acts to allow schools to deposit completed school registers and roll books which are no longer required for administrative purposes with the Local Authority Archive Service. The Department will notify schools of any changes to the Acts in this regard.
- Pay, taxation and related school personnel service records should be retained indefinitely within the school.
- Where litigation may potentially arise in the future (e.g. in relation to accidents/personal injuries involving school personnel/students or accidents occurring on school property), the relevant records should be retained until the possibility of litigation ceases.

Note: The statute of limitations in relation to personal injuries is currently two years. The limitation period for other causes of action varies, but in most cases is not greater than six years. A limitation period does not begin to run until the person concerned acquires knowledge of the facts giving rise to the claim. In the case of minors, the limitation period does not begin to run until they reach their 18th birthday or later if the date of knowledge post dates their 18th birthday. While schools may wish to draw up their own policies as to how long to retain such records, it would appear prudent not to destroy records likely to be relevant in litigation at least until the **six year limitation period** has expired.

In line with the above, it is suggested that the information on student files might, as a general rule, be retained for a period of six years after the student has completed the Senior Cycle and/or reached the age of 18. In Gaelscoil Bhrian Bóirimhe files are held until the students reach the age of 21.

8. *Give a copy of his/her personal data to that individual on request*

On making an access request any individual (subject to the restrictions in Notes A and B below) about whom you keep personal data, is entitled to:

- a copy of the data which is kept about him/her
- know the purpose/s for processing his/her data
- know the identity of those to whom the data is disclosed
- know the source of the data, unless it is contrary to public interest
- know the logic involved in automated decisions
- a copy of any data held in the form of opinions, except where such opinions were given in confidence.

To make an access request, an individual must:

- apply in writing
- give any details which might be needed to help identify him/her and locate all the information you may keep about him/her

There are a number of exceptions to the general rule of Right of Access, including those specified in Notes A and B below.

Handling access requests:

- The Principal is the named person responsible for handling access requests.
- There are procedures in place to provide applicants with access to personal data about themselves in accordance with the Data Protection Acts as detailed above.
- A signed letter of request along with photo I.D. is required to prove identity in order to access personal data.
- A record of the outcome of any legal proceedings which may limit the right of one or both parents to access information about their child is kept in the child's file in the office
Note: If spouses are separated and one of them has obtained an order for custody but both of them remain guardians, then both of them are entitled to be involved in important decisions which affect the child.
- All relevant manual files and computers are checked for the data in respect of which the access request is made.
- Incidents where any inaccurate information is identified by the individual on whom the data is kept is erased and/or rectified within 40 days of the request being made.
- Information is supplied promptly and within 40 days of receiving the request or, in respect of examinations data, within 60 days of receiving the request or 60 days of first publication of the results (whichever is the later).
- Information is provided in a form which is clear to the ordinary person.
- The individual is informed within 40 days of the request if no information is held on them.

Note A: Access requests by students

- Students aged 18 and over are entitled to access their personal information in accordance with the Data Protection Acts.
- Students under 18 years of age can be given access to their personal information, depending on the age of the student and the nature of the record i.e. it is suggested that:
 - if the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access
 - if the record is of a sensitive nature, it would be prudent to seek parental/guardian consent
 - if a student has some disability or medical condition that would impair his or her ability to understand the information, or if disclosure would be likely to be harmful to the individual concerned, parental/guardian consent should be sought.

Note B: Exceptions to note:

- Schools should note that data protection regulations prohibit the supply of:
 - health data to a patient in response to a request for access if that would cause serious harm to his or her physical or mental health. The regulations also provide that such data is to be communicated only by, or after consultation with, an appropriate "health professional", normally the patient's own doctor
 - personal data obtained in the course of carrying on social work if that would cause serious harm to the health or emotional condition of the data subject concerned. The regulations apply to social work carried on by Ministers, local authorities, the HSE or any other such bodies receiving financial assistance from public funds.

Links to Other Policies and to Curriculum Delivery

Identify any links to related school policies

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

The following policies may be among those considered:

- Child Protection Policy
- Guidance Plan
- Anti-Bullying Policy
- Substance Use Policy
- Code of Behaviour.

Identify any links to curriculum delivery

- SPHE (Appropriate/safe Internet Usage)

Implementation Arrangements, Roles and Responsibilities
--

The Principal will be assigned the role of co-ordinating implementation of the policy and for ensuring that staff who handle or have access to personal data are familiarised with their data protection responsibilities.

School administrative staff will have a key role in implementing the policy and should be provided with a copy of the policy and other relevant information. Teaching staff could be provided, at the minimum, with a broad outline of the policy, including a summary of the eight rules of data protection.

Ratification & Communication

- The board of management officially ratified the policy in November 2019.
- Shared with the school staff at staff meeting. Available on the school's website for parents and guardians and form to be signed by said parties when they register their child for the first time. Current parents are required to sign said form before December 2019.

Implementation Date

The policy will apply from December 2019.

Monitoring the implementation of the policy

The implementation of the policy will be monitored by the Principal and Deputy Principal

Reviewing and evaluating the policy

The policy will be reviewed in two year intervals.

- Some practical indicators which will be used to gauge the impact and effectiveness of the policy are:
 - Students, staff and parents/guardians are aware of the policy
 - Requests for access to personal data are dealt with effectively
 - Personal data records are accurate
 - Personal data records are held securely
 - Personal data records are retained only for as long as necessary.

Signed by the Chairperson of the Board of Management on

25/11/19.

Signed: _____

Maire Z. Mhic