Scoil Bhride
Crosshaven, Co. Cork
t: 021 483 1646 m: 086 772 6326
e: secretary@scoilbhridecrosshaven.ie
w: www.scoilbhridecrosshaven.ie

Data Protection and Record-Keeping Policy
Scoil Bhríde
13910N

Contents
(Compliant with G.D.P.R. Requirements May 2018)

Scoil Bhríde
Date Protection and Recording Keeping Protocols

Introductory Statement

The Scoil Bhríde Data Protection and Record-Keeping Policy applies to the personal data held by Scoil Bhríde which is protected by the Data Protection Acts 1988 and 2003. It was re-drafted during the Spring/Summer term of 2018 to meet with the GDPR needs of May of that year. The entire school community was involved in drafting this policy, which was adopted by the Board in June 2018

The policy applies to all school staff, the Board of Management, Parents/ Guardians, students and others (including prospective or potential students and their parents/guardians and applicants for staff positions within the school) insofar as the measures under the policy relate to them. Data will be stored securely, so that confidential information is protected in compliance with relevant legislation. This policy sets out the manner in which personal data and sensitive personal data will be protected by the school.

Data Protection Principles

The school is a *data controller* of *personal data* relating to its past, present and future staff, students, parents/guardians and other members of the school community. As such, the school is obliged to comply with the principles of data protection set out in the Data Protection Acts 1988 and 2003 which can be summarised as follows:

- **Obtain and process *Personal Data* fairly**: Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection Acts and the terms of this Data Protection Policy. The information will be obtained and processed fairly.

- **Keep it only for one or more specified and explicit lawful purposes**: The School will inform individuals of the reasons they collect their data and will inform individuals of the uses to which their data will be put. All information is kept with the best interest of the individual in mind at all times.

- **Process it only in ways compatible with the purposes for which it was given initially**: Data relating to individuals will only be processed in a manner consistent with the purposes for which it was gathered. Information will only be disclosed on a need to know basis, and access to it will be strictly controlled.

- **Keep *Personal Data* safe and secure**: Only those with a genuine reason for doing so may gain access to the information. Sensitive Personal Data is securely stored under lock and key in the case of manual records and

protected with firewall software and password protection in the case of electronically stored data. Portable devices storing personal data (such as laptops) should be encrypted and password protected before they are removed from the school premises. Confidential information will be stored securely and in relevant circumstances, it will be placed in a separate file which can easily be removed if access to general records is granted to anyone not entitled to see the confidential data.

- **Keep Personal Data accurate, complete and up-to-date**: Students, parents/guardians, and/or staff should inform the school of any change which the school should make to their personal data and/or sensitive personal data to ensure that the individual's data is accurate, complete and up-to-date. Once informed, the school will make all necessary changes to the relevant records. The principal may delegate such updates/amendments to another member of staff. However, records must not be altered or destroyed without proper authorisation. If alteration/correction is required, then a note of the fact of such authorisation and the alteration(s) to be made to any original record/ documentation should be dated and signed by the person making that change.

- **Ensure that it is adequate, relevant and not excessive**: Only the necessary amount of information required to provide an adequate service will be gathered and stored.

- **Retain it no longer than is necessary for the specified purpose or purposes for which it was given**: As a general rule, the information will be kept for the duration of the individual's time in the school. Thereafter, the school will comply with DES guidelines on the storage of Personal Data and Sensitive Personal Data relating to a student. In the case of members of staff, the school will comply with both DES guidelines and the requirements of the Revenue Commissioners with regard to the retention of records relating to employees. The school may also retain the data relating to an individual for a longer length of time for the purposes of complying with relevant provisions of law and or/defending a claim under employment legislation and/or contract and/or civil law.

- **Provide a copy of their *personal data* to any individual, on request**: Individuals have a right to know what personal data/sensitive personal data is held about them, by whom, and the purpose for which it is held.

Purpose of the Policy

The Data Protection Acts 1988 and 2003 apply to the keeping and processing of *Personal Data*, both in manual and electronic form. The purpose of this policy is to assist the school to meet its statutory obligations, to explain those obligations to School staff, and to inform staff, students and their parents/guardians how their data will be treated. The policy also aims to ensure data is maintained in a confidential manner and sets out the procedures in applying for access to such records by parents, students, staff and third parties.

The policy applies to all school staff, the Board of Management, Parents/ Guardians, students and others (including prospective or potential students and their parents/guardians, and applicants for staff positions within the school) insofar as the school handles or processes their *Personal Data* in the course of their dealings with the school.

Definition of Data Protection Terms

In order to properly understand the school's obligations, there are some key terms which should be understood by all relevant school staff:

Data means information in a form that can be processed. It includes both *automated data* (e.g. electronic data) and *manual data*. *Automated data* means any information on computer, or information recorded with the intention that it be *processed* by computer. *Manual data* means information that is kept/recorded as

part of a *relevant filing system* or with the intention that it 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, quickly and easily accessible.

Personal Data means 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 the Data Controller i.e. the Board of Management of Scoil Bhríde

Sensitive Personal Data refers to *Personal Data* regarding a person's

- racial or ethnic origin, political opinions or religious or philosophical beliefs
- membership of a trade union
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence or
- any proceedings for an offence committed or alleged to have been committed by the person, the disposal of such proceedings or the sentence of any court in such proceedings, criminal convictions or the alleged commission of an offence.

Data Controller for the purpose of this policy is the Board of Management of Scoil Bhríde.

Rationale

In addition to its legal obligations under the broad remit of educational legislation, the school has a legal responsibility to comply with the Data Protection Acts, 1988 and 2003.

This policy explains what sort of data is collected, why it is collected, for how long it will be stored and with whom it will be shared. As more and more data is generated electronically and as technological advances enable the easy distribution and retention of this data, the challenge of meeting the school's legal responsibilities has increased.

Scoil Bhríde takes its responsibilities under data protection law very seriously and wishes to put in place safe practices to safeguard individual's personal data. It is also recognised that recording factual information accurately and storing it safely facilitates an evaluation of the information, enabling the principal and board of management to make decisions in respect of the efficient running of the School. The efficient handling of data is also essential to ensure that there is consistency and continuity where there are changes of personnel within the school and board of management.

Other Legal Obligations

Implementation of this policy takes into account the school's other legal obligations and responsibilities. Some of these are directly relevant to data protection. ***For example:***

- 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 their education

- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School

- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring

- 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 School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training)

- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers ("SENOs")) such information as the Council may from time to time reasonably request

- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body

- Under Section 26(4) of the Health Act, 1947 a School shall cause all reasonable facilities (including facilities for obtaining names and addresses of pupils attending the school) to be given to a health authority who has served a notice on it of medical inspection, e.g. a dental inspection

- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

Relationship to School Ethos

Scoil Bhríde promotes openness and co-operation between staff, parents and pupils as a means towards providing the caring environment through which a child can develop and grow to his full potential. Scoil Bhríde is an all girl's Primary School founded on the Presentation philosophy of Education and Catholic faith. We strive to proactively nurture and educate each child to her fullest potential and at every stage of her development. We believe in striking balance

and we encourage the cultivation of strong relationships within the school and community.

We aim to achieve these goals while respecting the privacy and data protection rights of students, staff, Parents/Guardians and others who interact with us. The school wishes to achieve these aims/missions while fully respecting individuals' rights to privacy and rights under the Data Protection Acts.

Personal Data

The *Personal Data* records held by the school **may** include:

Staff Records:

(a) **Categories of staff data**: As well as existing members of staff (and former members of staff), these records may also relate to applicants applying for positions within the school, trainee teachers and teachers under probation. These staff records may include:

- Name, address and contact details, PPS number
- Original records of application and appointment to promotion posts
- Details of approved absences (career breaks, parental leave, study leave etc.)
- Details of work record (qualifications, classes taught, subjects etc.)
- Details of any accidents/injuries sustained on school property or in connection with the staff member carrying out their school duties
- Records of any reports the school (or its employees) have made in respect of the staff member to State departments and/or other agencies under mandatory reporting legislation and/or child-safeguarding guidelines (subject to the DES Child Protection Procedures).

(b) **Purposes**: Staff records are kept for the purposes of:

- the management and administration of school business (now and in the future)
- to facilitate the payment of staff, and calculate other benefits/ entitlements (including reckonable service for the purpose of calculation of pension payments, entitlements and/or redundancy payments where relevant)
- to facilitate pension payments in the future
- human resources management
- recording promotions made (documentation relating to promotions applied for) and changes in responsibilities etc.
- to enable the school to comply with its obligations as an employer including the preservation of a safe, efficient working and teaching environment (including complying with its responsibilities under the Safety, Health and Welfare At Work Act. 2005)
- to enable the school to comply with requirements set down by the Department of Education and Skills, the Revenue Commissioners, the National Council for Special Education, TUSLA, the HSE, and any other governmental, statutory and/or regulatory departments and/or agencies
- and for compliance with legislation relevant to the school.

(c) **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. Where the data is maintained electronically, such data should be stored on a password protected system with the appropriate firewall software installed.

(d) Security: Manual data should be stored in a locked, secure cabinet. Where data is stored electronically or automated data, the School should ensure that there are appropriate level of passwords, encryption and firewall software in place in order to maintain confidentiality and limit access to authorised personnel only.

Student Records:

(a) **Categories of student data**: These **may** include:

- Information which may be sought and recorded at enrolment and may be collated and compiled during the course of the student's time in the school. These records may include:
  - name, address and contact details, PPS number
  - date and place of birth
  - names and addresses of parents/guardians and their contact details (including any special arrangements with regard to guardianship, custody or access)
  - religious belief
  - racial or ethnic origin
  - membership of the Traveller community, where relevant
  - whether they (or their parents) are medical card holders
  - whether English is the student's first language and/or whether the student requires English language support
  - any relevant special conditions (e.g. special educational needs, health issues etc.) which may apply
- Information on previous academic record (including reports, references, assessments and other records from any previous school(s) attended by the student.
- Psychological, psychiatric and/or medical assessments.
- Behavioural Plans for SEN students.
- Attendance records.
- Photographs and recorded images of students (including at school events and noting achievements). See the template "Guidance on Taking and Using Images of Children in Schools"
- Academic record – subjects studied, class assignments, examination results as recorded on official School reports
- Records of significant achievements
- Whether the student is repeating the Leaving Certificate
- Whether the student is exempt from studying Irish
- Records of disciplinary issues/investigations and/or sanctions imposed
- Garda vetting outcome record (where the student is engaged in work experience organised with or through the school/ETB which requires that they be Garda vetted)
- Other records e.g. records of any serious injuries/accidents etc. (Note: it is advisable to inform parents that a particular incident is being recorded).
- Records of any reports the school (or its employees) have made in respect of the student to State departments and/or other agencies under mandatory reporting legislation and/or child safeguarding guidelines (subject to the DES Child Protection Procedures).
- Letters to outside agencies (Social Work, HSE, NEPS, DES, NCSE) and correspondence with parents.

(b) **Purposes**: The purposes for keeping student records are:

- to enable each student to develop to their full potential
- to comply with legislative or administrative requirements
- to ensure that eligible students can benefit from the relevant additional teaching or financial supports
- to support the provision of religious instruction

- to enable parents/guardians to be contacted in the case of emergency or in the case of school closure, or to inform parents of their child's educational progress or to inform parents of school events etc.
- to meet the educational, social, physical and emotional requirements of the student
- photographs and recorded images of students are taken to celebrate school achievements, compile yearbooks, establish a school website, record school events, and to keep a record of the history of the school. Such records are taken and used in accordance with the school's "Guidance for Taking and Using Images of Pupils in Schools" (see template)
- to ensure that the student meets the school's admission criteria
- to ensure that students meet the minimum age requirements for their course,
- to ensure that any student seeking an exemption from Irish meets the criteria in order to obtain such an exemption from the authorities
- to furnish documentation/ information about the student to the Department of Education and Skills, the National Council for Special Education, TUSLA, and other Schools etc. in compliance with law and directions issued by government departments
- to furnish, when requested by the student (or their parents/guardians in the case of a student under 18 years) documentation/information/ references to third-level educational institutions and/or prospective employers
- In respect of a work experience placement, (where that work experience role requires that the student be Garda vetted) the School will assist the student in obtaining their Garda vetting outcome (with the consent of the student and their parent/guardian) in order to furnish a copy of same (with the consent of the student and the student's parent/guardian) to the work experience employer.

(c) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Where the data is maintained electronically, such data should be stored on a password protected system with the appropriate firewall software installed. Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security: Manual Data should be stored in a locked filing cabinet. Where data is stored electronically or automated data, the School should ensure that there are the appropriate level of passwords, encryption and firewall software in place in order to maintain confidentiality and limit access to authorised personnel only.

Board of Management Records

(a) **Categories of** board of management data: These may include:

- Name, address and contact details of each member of the board of management (including former members of the board of management)
- Records in relation to appointments to the Board
- Minutes of Board of Management meetings and correspondence to the Board which may include references to particular individuals.
-

(b) Purposes: To enable the Board of Management to operate in accordance with the Education Act 1998 and other applicable legislation and to maintain a record of board appointments and decisions.

(a) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Where the data is maintained

electronically, such data should be stored on a password protected system with the appropriate firewall software installed. Employees are required to maintain the confidentiality of any data to which they have access.

(b) Security: Manual Data should be stored in a locked filing cabinet. Where data is stored electronically or automated data, the Board of Management should ensure that there are the appropriate level of passwords, encryption and firewall software in place in order to maintain confidentiality and limit access to authorised personnel only.

Other Records

The school will hold other records relating to individuals. The format in which these records will be kept are manual record (personal file within a relevant filing system), and/or computer record (database). Some examples of the type of other records which the school will hold are set out below (this list is not exhaustive):

Creditors

(a) **Categories of data**: the school may hold some or all of the following information about creditors (some of whom are self-employed individuals):
- name
- address
- contact details
- PPS number
- tax details
- bank details and
- amount paid.

(b) **Purposes**: This information is required for routine management and administration of the school's financial affairs, including the payment of invoices, the compiling of annual financial accounts and complying with audits and investigations by the Revenue Commissioners.

(c) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Where the data is maintained electronically, such data should be stored on a password protected system with the appropriate firewall software installed. Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security: Manual Data should be stored in a locked filing cabinet. Where data is stored electronically or automated data, the School should ensure that there are the appropriate level of passwords, encryption and firewall software in place in order to maintain confidentiality and limit access to authorised personnel only.

Charity tax-back forms

(a) **Categories of data**: the school may hold the following data in relation to donors who have made charitable donations to the school:
- name
- address
- telephone number
- PPS number
- tax rate
- signature and
- the gross amount of the donation.

(b) **Purposes**: Schools are entitled to avail of the scheme of tax relief for donations of money they receive. To claim the relief, the donor must complete a certificate (CHY2) and forward it to the school to allow it to claim the grossed up amount of tax associated with the donation. The

information requested on the appropriate certificate is the parents name, address, PPS number, tax rate, telephone number, signature and the gross amount of the donation. This is retained by the School in the case of audit by the Revenue Commissioners.

(c) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Where the data is maintained electronically, such data should be stored on a password protected system with the appropriate firewall software installed. Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security: Manual Data should be stored in a locked filing cabinet. Where data is stored electronically or automated data, the School should ensure that there are the appropriate level of passwords, encryption and firewall software in place in order to maintain confidentiality and limit access to authorised personnel only.

CCTV Images/Recordings (Refer to the Scoil Bhríde CCTV Policy)

(a) **Categories**: CCTV is installed in some schools, externally i.e. perimeter walls/fencing and internally as detailed in the CCTV Policy. These CCTV systems may record images of staff, students and members of the public who visit the premises.

(b) **Purposes**: Safety and security of staff, students and visitors and to safeguard school property and equipment.

(c) **Location**: Cameras are located externally and internally as detailed in the CCTV Policy. Recording equipment is located beside the Principal's office in the school.

(d) **Security**: Access to images/recordings is restricted to the principal & deputy principal of Scoil Bhríde. Hard disk recordings are retained for 30 days, except if required for the investigation of an incident. Images/ recordings may be viewed or made available to An Garda Síochána pursuant to section 8 Data Protection Acts 1988 and 2003.

Assessment/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 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 subject choices and levels. 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.

(c) **Location**: In a secure, locked filing cabinet that only personnel who are authorised to use the data can access. Where the data is maintained electronically, such data should be stored on a password protected system with the appropriate firewall software installed. Employees are required to maintain the confidentiality of any data to which they have access.

(d) Security: Manual Data should be stored in a locked filing cabinet. Where data is stored electronically or automated data, the School should ensure that there are the appropriate level of passwords, encryption and firewall

software in place in order to maintain confidentiality and limit access to authorised personnel only.

Links to Other Policies of Scoil Bhríde

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 and Record-Keeping Policy and any implications which it has for them shall be addressed.

The following policies may be among those considered:

- Child Protection Policy
- Anti-Bullying Policy
- Code of Behaviour
- Mobile Phone Code
- Admissions/Enrolment Policy
- CCTV Policy
- Substance Use Policy
- ICT Acceptable Usage Policy
- SPHE/CSPE etc.

Destruction of Personal Data

The destruction of records will be carried out by authorised personnel only and using a shredder to ensure the upmost of confidentiality at all times.

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 Request

(a) Section 3 Access Request

Under Section 3 of the Data Protection Acts, an individual has the right to be informed whether the school holds data/information about them and to be given a description of the data together with details of the purposes for which their data is being kept. The individual must make this request in writing and the data controller will accede to the request within 21 days.

The right under Section 3 must be distinguished from the much broader right contained in Section 4, where individuals are entitled to a copy of their data.

(b)Section 4 Access Request

Individuals are entitled to a copy of their personal data on written request.

- The individual is entitled to a copy of their personal data (subject to some exemptions and prohibitions set down in Section 5 of the Data Protection Act)
- Request must be responded to within 40 days
- Fee may apply but cannot exceed €6.35
- Where a subsequent or similar request is made soon after a request has just been dealt with, it is at the discretion of the school as data controller to comply with the second request (no time limit but reasonable interval from the date of compliance with the last access request.) This will be determined on a case-by-case basis.
- No personal data can be supplied relating to another individual unless that third party has consented to the disclosure of their data to the applicant. Data will be carefully redacted to omit references to any other individual and only where it has not been possible to redact the data to ensure that the third party is not identifiable would the school refuse to furnish the data to the applicant.

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.

Implementing 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**
Sr. Anne Coffey	
Jim Nyhan	
Board of Management:	Data Controllers
Séamus O'Connor	
Principal:	Implementation of Policy
Miriam Long/Leah Weste	
Teaching personnel:	Awareness of responsibilities

Administrative personnel: Security, confidentiality

Aladdin/KD Systems

IT Providers: Security, encryption, confidentiality

Ratification and Communication

When the Data Protection Policy has been ratified by the board of management, it becomes the school's agreed Data Protection Policy. It should then be dated and circulated within the school community. The entire staff must be familiar with the Data Protection Policy and ready to put it into practice in accordance with the specified implementation arrangements. It is important that all concerned are made aware of any changes implied in recording information on students, staff and others in the school community.

Parents/Guardians, staff and students should be informed of the Data Protection Policy from the time of enrolment of the student e.g. by including the Data Protection and Record Keeping Policy Policy as part of the emailed 'Enrolment Pack', made available n the school website or by enclosing it/incorporating it as an appendix to the enrolment form.

Monitoring the Implementation of the Policy

The implementation of the policy shall be monitored by the principal and a sub-committee of the board of management.

At least one annual report should be issued to the board of management to confirm that the actions/measures set down under the policy are being implemented.

Reviewing and Evaluating the Policy

The Policy should be reviewed and evaluated at certain pre-determined times and as necessary. On-going review and evaluation should take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, Department of Education and Skills or the NEWB), legislation and feedback from parents/guardians, students, school staff and others. The policy should be revised as necessary in the light of such review and evaluation and within the framework of school planning.

Signed: …….

For and behalf of board of management

Date: May 2019

Scoil Bhride
Crosshaven, Co. Cork
t: 021 483 1646 m: 086 772 6326
e: secretary@scoilbhridecrosshaven.ie
w: www.scoilbhridecrosshaven.ie

Data Protection Statement
Scoil Bhríde
13910N

This statements for inclusion on relevant forms (e.g. Scoil Bhríde Enrolment Form, AUP) when personal information is being requested

Personal Data on this Form:

Scoil Bhríde is a data controller under the Data Protection Acts, 1988 and 2003. The personal data supplied on this form is required for the purposes of:

- student enrolment
- student registration
- allocation of teachers and resources to the school
- determining a student's eligibility for additional learning supports and transportation
- examinations
- school administration
- child welfare (including medical welfare)
- and to fulfil our other legal obligations.

School Contacting You

Please confirm if you are happy for us to contact you by SMS/text message and to call you on the telephone numbers provided and to send you emails for all the purposes of:

- sports days
- parent teacher meetings
- school concerts/events
- to notify you of school closure (e.g. where there are adverse weather conditions)

- to notify you of your child's non-attendance or late attendance or any other issues relating to your child's conduct in school
- to communicate with you in relation to your child's social, emotional and educational progress and to contact you in the case of an emergency.

Tick box if "YES" you agree with these uses

Use your email address to alert you to these issues? ☐

Use your mobile phone number to send you SMS texts to alert you to these issues? ☐

Use your mobile phone/landline number to call you to alert you to these issues? ☐

Please note: Scoil Bhríde reserves the right to contact you in case of an emergency relating to your child, regardless of whether you have given your consent.

School sending you direct marketing

We would like to send you emails/SMS text messages or call you or write to you at your home address to inform you of special offers or promotions by certain third parties involved in the supply of school books/stationery and school uniform supplies etc. (e.g. High Street Books/4orm Uniforms). Do you give your consent for us to do each of the following:

Tick box if "yes" you agree with these uses

Use your email address to alert you to these offers? ☐

Use your mobile phone number to send you SMS texts in relation to these offers? ☐

Use your mobile phone/landline number to call you in relation to these offers? ☐

Use your address to send you written letters/brochures in relation to these offers? ☐

While the information provided will generally be treated as private to *Scoil Bhríde* and will be collected and used in compliance with the Data Protection Acts 1988 and 2003, from time to time it may be necessary for us to transfer your personal data on a private basis to other bodies (including the Department of Education & Skills, the Department of Social Protection, An Garda Síochána, the Health Service Executive, Tusla (CFA), social workers or medical practitioners, the National Educational Welfare Board, the National Council for Special Education, any Special Education Needs Organiser, the National Educational Psychological Service, or (where the student is transferring) to another school). We rely on parents/guardians and students to provide us with accurate and complete information and to update us in relation to any change in the information provided. Should you wish to update or access your/your child's personal data, you should write to the school principal requesting an Access Request Form.

Scoil Bhríde Data Protection and Record-Keeping Policy:

A copy of the full Data Protection Policy is enclosed in this Enrolment Pack, and you and your child should read it carefully. When you apply for enrolment, you will be asked to sign that you consent to your data/your child's data being collected, processed and used in accordance with this Data Protection Policy during the course of their time as a student in the school. Where the student is over 18 years old, they will be asked to sign their consent to this.

Photographs of Students:

The school maintains a database of photographs of school events held over years. It has become customary to take photos of students engaged in activities and events in the interest of creating a pictorial as well as historical record of life at the school. Photographs may be published on our school website or in brochures, yearbooks, newsletters, local and national newspapers and similar school-related productions. In the case of website photographs, student names will not appear on the website as a caption to the picture. If you or your child wish to have his/ her photograph removed from the school website, brochure, yearbooks, newsletters etc. at any time, you should write to the school principal.

Consent *(tick one only)*

1. If you are happy to have your child's photograph taken as part of school activities and included in all such records, tick here c
2. If you would prefer not to have your child's photograph taken and included in such records, please tick here c
3. If you are happy for your child's photograph to be taken and included, as *1.* above, but would prefer not to have images of your child appear on the school website, in school brochures, yearbooks, newsletters etc., please tick here. c

Signed: _____
Parent/Guardian (1)

Signed: _____
Parent/Guardian (2)

Date: _____

Scoil Bhride
Crosshaven, Co. Cork
t: 021 483 1646 m: 086 772 6326
e: secretary@scoilbhridecrosshaven.ie
w: www.scoilbhridecrosshaven.ie

Data Access Request Form
Scoil Bhríde
13910N

Date issued to data subject:

Access Request Form: Request for a copy of Personal Data under the Data Protection Act 1988 and Data Protection (Amendment) Act 2003

Important: Proof of Identity must accompany this Access Request Form (eg. official/State photographic identity document such as driver's licence, passport).

A fee of €6.35 must accompany this Access Request Form if it is a Section 4 Data Access Request together with proof of identity (eg. official/State photographic identity document such as driver's licence, passport).

Full Name	
Maiden Name *(if name used during* your school duration*)*	
Address	
Contact number *	Email addresses *

** We may need to contact you to discuss your access request*

Please tick the box which applies to you:

Student	Parent/Guardian of student	Former Student	Current Staff	Former Staff
o	o	o	o	o
Age/ Year group/ class:	Name of Student:	Insert Year of leaving:	Insert Years From/To:	

Section 3 Data Access Request:

I, ……..[insert name] wish to be informed whether or not Scoil Bhride holds personal data about me/my child and to be provided with a description of this data and to be informed of the purpose for holding such data. I am making this access request under **Section 3** of the Data Protection Acts.

c

OR

Section 4 Data Access Request:

I, …….. [insert name] wish to make an access request for a copy of any personal data that Scoil Bhride holds about me/my child. I am making this access request under **Section 4** of the Data Protection Acts.

c

Section 4 Data Access Request only: I attach €6.35 c

Any other information relevant to your access request (e.g. if requesting images/ recordings made by CCTV, please state the date, time and location of the images/ recordings (otherwise it may be very difficult or impossible for Scoil Bhride to locate the data).

Signed …… Date ……

Checklist: Have you:

1) Completed the Access Request Form in full? Y/N
2) Included a cheque or postal order made payable to <*name of school*> in the amount of €6.35 where a Section 4 request is made? (Please do not send us €6.35 if you are making a request under section 3. There is no administration charge for a section 3 request, and if you send us a cheque, it will be returned to you). Y/N
3) Signed and dated the Access Request Form? Y/N
4) Included a photocopy of official/State photographic identity document (driver's licence, passport etc.)*. Y/N

***Note to School**: the school should satisfy itself as to the identity of the individual and make a note in the school records that identity has been provided, but the school should not retain a copy of the identity document.

Please return this form to the relevant address: **To the Chairperson of Board of Management, Scoil Bhríde, Crosshaven, Co-Cork.**

Scoil Bhride
Crosshaven, Co. Cork
t: 021 483 1646 m: 086 772 6326
e: secretary@scoilbhridecrosshaven.ie
w: www.scoilbhridecrosshaven.ie

Personal Data Security Breach Code of Practice
Scoil Bhríde
13910N

Purpose of Code of Practice

This Code of Practice applies to Scoil Bhríde as *data controller(1).* This Code of Practice will be:

1. available on the school website
2. circulated to all appropriate *data processors*.
3. shall be advised to staff at induction and at periodic staff meeting(s) or training organised by the school.

Obligations under Data Protection

Scoil Bhríde as data controller and appropriate data processors so contracted, are subject to the provisions of the Data Protection Acts, 1988 and 2003 and exercise due care and attention in collecting, processing and storing personal data and sensitive personal data provided by data subjects for defined use.

The school has prepared a **Data Protection and Record-Keeping Policy** and monitors the implementation of this policy at regular intervals. The school retains records (both electronic and manual) concerning personal data in line with its **Data Protection and Record-Keeping Policy** and seeks to prioritise the safety of personal data and particularly sensitive personal data, so that any risk of unauthorized disclosure, loss or alteration of personal data is avoided.

Protocol for action in the event of breach

In circumstances where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the school will follow the following protocol**:**

1. The school will seek to contain the matter and mitigate any further exposure of the personal data held. Depending on the nature of the threat to the personal data, this may involve a quarantine of some or all PCs, networks etc. and requesting that staff do not access PCs, networks etc. Similarly, it may involve a quarantine of manual records storage area/s and other areas as may be appropriate. By way of a preliminary step, an audit of the records held or backup server/s should be undertaken to ascertain the nature of what personal data may potentially have been exposed.
2. Where data has been "damaged" (as defined in the Criminal Justice Act 1991, e.g. as a result of hacking), the matter must be reported to An Garda Síochána. Failure to do so will constitute a criminal offence in itself ("withholding information") pursuant to section 19 Criminal Justice Act, 2011. The penalties for withholding information include a fine of up to €5,000 or 12 months' imprisonment on summary conviction.
3. Where the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the school may conclude that there is no risk to the data and therefore no need to

inform data subjects or contact the Office of the Data Protection Commissioner. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

4. Depending on the nature of the personal data at risk and particularly where sensitive personal data may be at risk, the assistance of An Garda Síochána should be immediately sought. This is separate from the statutory obligation to report criminal damage to data arising under section 19 Criminal Justice Act 2011 as discussed at (2) above.

5. Contact should be immediately made with the data processor responsible for IT support in the school.

6. In addition and where appropriate, contact may be made with other bodies such as the HSE, financial institutions etc.

7. Reporting of incidents to the Office of Data Protection Commissioner: All incidents in which personal data (and sensitive personal data) has been put at risk shall be reported to the Office of the Data Protection Commissioner as soon as the school becomes aware of the incident (or within 2 working days thereafter), save in the following circumstances:

    - When the full extent and consequences of the incident have been reported without delay directly to the affected data subject(s) **and**
    - The suspected breach affects no more than 100 data subjects **and**
    - It does not include sensitive personal data or personal data of a financial nature[1].

   Where all three criteria are not satisfied, the school shall report the incident to the Office of the Data Protection Commissioner within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident (see further details below). Where no notification is made to the Office of the Data Protection Commissioner, the school shall keep a summary record of the incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record shall comprise a brief description of the nature of the incident and an explanation why the school/ ETB did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records shall be provided to the Office of the Data Protection Commissioner upon request.
8. The school shall gather a small team of persons together to assess the potential exposure/loss. This team will assist the Principal of the school (and the school's DP Compliance Officer) with the practical matters associated with this protocol.

[1] 'personal data of a financial nature' means an individual's last name, or any other information from which an individual's last name can reasonably be identified, in combination with that individual's account number, credit or debit card number.

9. The team will, under the direction of the Principal, give immediate consideration to informing those affected[2]. At the direction of the Principal, the team shall:
    - Contact the individuals concerned (whether by phone/email etc.) to advise that an unauthorised disclosure/loss/destruction or alteration of the individual's personal data has occurred.
    - Where possible and as soon as is feasible, the *data subjects* (i.e. individuals whom the data is about) should be advised of
        - the nature of the data that has been potentially exposed/ compromised;
        - the level of sensitivity of this data and
        - an outline of the steps the school/ETB intends to take by way of containment or remediation.
    - Individuals should be advised as to whether the school intends to contact other organisations and/or the Office of the Data Protection Commissioner.
    - Where individuals express a particular concern with respect to the threat to their personal data, this should be advised back to the principal who may, advise the relevant authority e.g. Gardaí, HSE etc.
    - Where the data breach has caused the data to be "damaged" (e.g. as a result of hacking), the principal/CEO of the ETB shall contact An Garda Síochána and make a report pursuant to section 19 Criminal Justice Act 2011.
    - The principal/CEO of the ETB shall notify the insurance company which the school/ETB is insured and advise them that there has been a personal data security breach.
10. Contracted companies operating as data processors: Where an organisation contracted and operating as a *data processor* on behalf of the school/ETB becomes aware of a risk to personal/sensitive personal data, the organisation will report this directly to the school/ETB as a matter of urgent priority. In such circumstances, the principal of the school should be contacted directly (and in the case of an ETB school, both the principal and the Chief Executive Officer should be contacted). This requirement should be clearly set out in the data processing agreement/contract in the appropriate data protection section in the agreement.
10. A full review should be undertaken using the template Compliance Checklist and having regard to information ascertained deriving from the experience of the data protection breach. Staff should be apprised of any changes to the Personal Data Security Breach Code of Practice and of upgraded security measures. Staff should receive refresher training where necessary.

Further advice:
What may happen arising from a report to the Office of Data Protection Commissioner?

- Where any doubt may arise as to the adequacy of technological risk-mitigation measures (including encryption), the school/ETB shall

[2] Except where law enforcement agencies have requested a delay for investigative purposes. Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows. Where <Name of School/ETB> receives such a direction from law enforcement agencies, they should make careful notes of the advice they receive (including the date and the time of the conversation and the name and rank of the person to whom they spoke). Where possible, <Name of School/ETB> should ask for the directions to be given to them in writing on letter-headed notepaper from the law enforcement agency (eg. An Garda Siochána), or where this is not possible, <Name of School/ETB> should write to the relevant law enforcement agency to the effect that "we note your instructions given to us by your officer [insert officer's name] on XX day of XX at XXpm that we were to delay for a period of XXX/until further notified by you that we are permitted to inform those affected by the data breach."

report the incident to the Office of the Data Protection Commissioner within **two working days** of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be by e-mail, telephone or fax and shall **not** involve the communication of personal data.

- The Office of the Data Protection Commissioner will advise the school/ETB of whether there is a need for the school/ETB to compile a detailed report and/or for the Office of the Data Protection Commissioner to carry out a subsequent investigation, based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.
- Should the Office of the Data Protection Commissioner request the school/ETB to provide a detailed written report into the incident, the Office of the Data Protection Commissioner will specify a timeframe for the delivery of the report into the incident and the information required. Such a report should reflect careful consideration of the following elements:

    - the amount and nature of the personal data that has been compromised
    - the action being taken to secure and/or recover the personal data that has been compromised
    - the action being taken to inform those affected by the incident or reasons for the decision not to do so
    - the action being taken to limit damage or distress to those affected by the incident
    - a chronology of the events leading up to the loss of control of the personal data; and
    - the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the school/ETB has not already done so. If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.