

# **SCOIL BHRÍDE BOYS NS**

## **COMPUTER SYSTEMS ACCEPTABLE USAGE POLICY**

### **1. PURPOSE**

Scoil Bhríde B.N.S owns and operates a variety of computing systems. It is intended that these computer systems will be used by the staff and students (**Users**) of Scoil Bhríde B.N.S as a means of accessing content that supports the delivery of the National Primary Curriculum to all students.

This document establishes rules and regulations that serve to define acceptable use of these computer systems. Unacceptable use of the computer systems in Scoil Bhríde B.N.S is deemed to be - any behaviour that seeks to contravene the rules and regulations that are clearly set out in this policy document. Staff members and/or students who engage in unacceptable use of the computer systems in Scoil Bhríde B.N.S can and may be subject to the revocation of computing privileges, as well as disciplinary or legal sanctions.

### **2. AUDIENCE & AGREEMENT**

All users of Scoil Bhríde's B.N.S computing systems must read, understand, and comply with the policies outlined in this document, as well as any additional guidelines established by the National Centre for Technology in Education (NCTE). Such guidelines will be reviewed by the school and may become subject to Board approval as a policy or procedure to be included in the school plan. **When using any of these systems, users agree that they will comply with these policies.**

### **3. RIGHTS**

Scoil Bhríde B.N.S reserves all rights to the computing systems that it owns and operates. These procedures shall not be construed as a waiver of any rights of the school, nor shall they conflict with applicable acts of law.

### **4. PRIVILEGES**

Access and privileges on Scoil Bhríde's B.N.S computing systems are assigned and managed by the ICT Special Duties Teacher. Eligible individuals may become authorised users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system by the ICT Special Duties Teacher.

The ICT Special Duties Teacher must approve all access to the School's computer resources, including the issuing of accounts and related passwords.

Users may not, under any circumstances, transfer or confer these privileges to other individuals. Others shall not use any account assigned to an individual without express permission from the ICT Special Duties Teacher. The authorised user is responsible for the proper use of the system, including any password protection.

## **5. RESPONSIBILITIES**

### **ICT Special Duties Teacher:**

This document establishes the need for an ICT Special Duties Teacher. The task of this ICT Special Duties Teacher is to:

- In conjunction with the Board of Management, secure an annual budget and provide an annual budget breakdown.
- Ensure that there is an ongoing program of staff development and support.
- Regularly review hardware, software and ICT training needs.
- Co-ordinate, where necessary, with resource leaders in other curriculum areas, particularly in respect to software purchases.

### **Staff Members:**

Staff members of Scoil Bhríde B.N.S are responsible for fostering:

- An environment in which access to all School computing resources are shared equitably between users. The ICT Special Duties Teacher sets minimum guidelines within which users must conduct their activities.
- An environment conducive to learning:
  - Users will not be permitted to have food or drink during computer lessons.
  - Disruptive behaviour will not be tolerated in any form. If any arises, the user responsible will be asked to close down their terminal and will be given alternative written work to complete at that time.

### **Students and Staff:**

A user who harasses, or makes defamatory remarks, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks shall bear sole responsibility for their actions. Users agree that Scoil Bhríde's B.N.S role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of said transmission by Scoil Bhríde B.N.S.

Some of the Scoil Bhríde's B.N.S computing systems provide access to outside networks, both public and private, which furnish electronic mail, information

services, bulletin boards, conferences, etc. Every effort is made to ensure that the users are not subjected to offensive or objectionable material in nature or content. . **Users (staff and students) are further advised that Scoil Bhríde B.N.S does not assume responsibility for the contents of any of these outside networks.** Scoil Bhríde BNS uses the NCTE monitoring system - Fortiguard which is in place to filter inappropriate sexual content, pornography, anti-religious content which undermines an individual's civil rights or any other age inappropriate material.

The users agree to comply with the acceptable use guidelines for whichever outside networks or services they may access through Scoil Bhríde B.N.S systems.

The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service). The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not Scoil Bhríde B.N.S which is acting solely as the information carrier.

#### **An Environment Free of Illegal or Malicious Acts:**

The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which (s)he is authorised, or any attempt to deprive other authorised users of resources or access to any of Scoil Bhríde's B.N.S computer system shall be regarded as malicious, and may be treated as an illegal act.

The user agrees to be bound by the terms and conditions laid down in the **Data Protection (Amendment) Act 2003** and the **Freedom of Information Act of 1997** and to inform themselves of their rights as citizens and their responsibilities under said acts.

Other legal/sector specific requirements need to be satisfied under the list of applicable Irish Laws as listed under the **Legislation** section of this document. All users agree to abide by the terms and conditions of these applicable Irish Laws.

#### **Secure Environment:**

When not in use the doors to all computer facilities must be kept locked.

Any user who finds a possible security lapse, or technical difficulty, on any system is obliged to report it to the ICT Special Duties Teacher. The system must not be used until the ICT Special Duties Teacher has investigated the problem.

Users are responsible for backup of their own data. The ICT Special Duties Teacher may from time to time schedule an overhaul and clean up of the

network. File owners will be notified of this necessary maintenance, in advance, if such notice is practical.

All users must become familiar with logging off the system and must do so at the end of every session. If so asked by their teacher, students must ensure that all systems are shut down, through the proper means, when they are finished using them.

## **6. ACCOUNTS**

Accounts will be issued and revoked solely by the ICT Special Duties Teacher. Others must not use an account assigned to an individual without express permission from the ICT Special Duties Teacher. The individual is responsible for the proper use of the account, including proper password protection.

The user is responsible for all work carried out through the account issued and for maintenance of files and folders created within said account.

## **7. CONFIDENTIALITY**

Programs and files are confidential unless they have been made available, with written permission, to other authorised individuals. The ICT Special Duties Teacher reserves the right to access all information stored on computers other than those used by senior management. File owners will be notified of file access and/or maintenance, in advance, if such notice is practical. When performing maintenance, every effort is made to ensure the privacy of a user's files. However, if policy violations are discovered, they will be reported immediately.

## **8. SYSTEM USAGE**

Electronic communications facilities (such as E-MAIL) are for school related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored.

The computer facilities may be used during out of class times by any student who has been deemed competent in computer usage by the ICT Special Duties Teacher.

Staff may use either the Computer room or trolley with their class group(s) during class time provided the appropriate class period(s) are recorded via the staff room notice board.

## **9. SYSTEM PERFORMANCE**

No one should deliberately attempt to degrade the performance of a computer system or to deprive authorised personnel of resources or access to any school computer.

## **10. UNAUTHORISED ACCESS**

Loopholes in computer security systems or knowledge of a special password should not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to systems for which proper authorization has not been given.

## **11. COPYRIGHT**

Computer software protected by copyright is not to be copied from, into, or by using Scoil Bhríde's B.N.S computing facilities, except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

## **12. VIRUS PROTECTION**

Computer viruses are items of software that attach themselves to other legitimate items of software or data, without the consent of the computer user, and are programmed to proliferate themselves onto other computers, often to cause disruption or damage. It is essential that all users play a part in protecting the network from the presence of viruses.

It is the policy of the school to run up to date virus protection software on all computers that are attached to the network. This software will automatically report the presence of most known viruses. Any user who receives an on-screen warning from this software (these are very clear and explicit) should stop all use of the computer immediately and report the occurrence to the ICT Special Duties Teacher or the teacher in charge.

Viruses can attach themselves easily to USB Keys/Sticks and this is one of the main ways in which they proliferate. All USB Keys/Sticks must be scanned by an Anti-Virus software programme prior to being connected to any computer system. The software used to prevent students from tampering with various computer settings will also, to some extent, prevent them from accessing USB Keys/Sticks. However this is not totally secure. Furthermore there are instances in which students and staff will want to transfer data to

and from the network on USB Keys/Sticks, e.g. as a means of submitting projects.

### **13. VIOLATIONS**

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of the rules and regulations outlined in this policy document. Suspected violations will be confidentially reported to the ICT Special Duties Teacher.

Violation of these rules and regulations will be dealt with in the same manner as violations or other school policies and may result in disciplinary action. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the school, and legal action. Violations of some of the rules and regulations contained in this policy document may constitute a criminal offence.

### **14. SCOIL BHRÍDE B.N.S STRATEGY**

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follow:

#### **General:**

- Internet sessions will always be supervised by a teacher.
- Uploading and downloading of non-approved software will not be permitted.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material. Filtering software and /or equivalent systems will be fully explained to all users.
- The school expects all parents/guardians to engage in teaching their children about responsible use of the Internet.
- The school will regularly monitor students' internet usage.
- Students and teachers will be provided with training in the area of internet safety.
- Virus protection software will be used and updated on a regular basis.
- The use of children's personal USB keys/sticks in school will not be permitted.
- Students will observe good "netiquette" (i.e. etiquette on the Internet) at all times and will not undertake any actions that may bring the school into disrepute.

### **World Wide Web:**

- Students will use the Internet for educational purposes only.
- Students will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials. Students will be familiar with copyright issues relating to online learning.
- Students will never disclose or publicise personal or school information especially on sites requiring e-commerce transactions.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

### **Email:**

- Students will only use approved class email accounts under supervision by or permission from a teacher.
- Students will not send or receive any material that is illegal, obscene, or defamatory or material that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone.
- Sending and receiving email attachments is subject to permission from their teacher.

### **Internet Chat:**

Students will only have access to chat rooms, discussion forums or other electronic communication forums that have been set up by the school.

- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.

### **School Website:**

We are privileged to have a portal on the world Wide Web that gives interested parties an insight into the life of Scoil Bhríde B.N.S. [www.scoilbhrídeb.com](http://www.scoilbhrídeb.com). It is envisaged that our students will contribute to the site and they will be given the opportunity to publish projects, artwork or school work on the World Wide Web. The publication of student work will be co-ordinated by a teacher. Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission. Digital photographs, audio or video clips of individual students will not be published on the school website without parental permission. Most photographs, audio and video clips featured on the school website will focus on group activities. Video clips may be password protected.

Personal student information including home address and contact details will be omitted from school web pages. Students will continue to own the copyright on any work published.

### **Technology Assisted Learning :**

In line with the school's policy on providing an inclusive learning environment for all students some of the computer systems in Scoil Bhríde B.N.S have been designated as assistive technology for those students with specific learning needs.

### **Legislation:**

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Child Trafficking and Pornography Act 1998
- Communications (Retention of Data) Act 2011
- Video Recordings Act 1989
- The Data Protection (Amendment) Act 2003
- Freedom of Information Act 1997
- Education for Persons with Special Educational Needs Act 2004
- Protections for Persons Reporting Child Abuse Act, 1998
- Education (Welfare) Act, 2000
- Children Act, 2001

### **Support Structures:**

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

### **Sanctions:**

**All sanctions will be in line with the School Code of Behaviour.**

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

## **15. ADDITIONAL GUIDELINES**

The ICT Special Duties Teacher will establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines will cover other items related to administration and implementation of a system that offers a first class learning experience to all users.

**16. ANNUAL REVIEW**

The aim of this Acceptable Use Policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. It is envisaged that school and Parent Association representatives will revise the AUP annually.

This version of the AUP was created on:

---

and was ratified by the Board of Management of Scoil Bhríde B.N.S on:

---

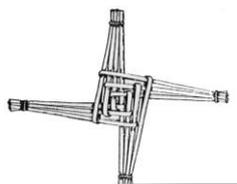
Signed:

---

**ICT Special Duties Teacher**

---

**Principal**



# **Scoil Bhríde Boys**

Church Avenue, Blanchardstown,  
Dublin 15 - ☎ 8201299

---

---

Dear Parent/Guardian,

## **RE: Internet Permission**

As part of the school's education programme we offer pupils supervised access to the Internet. This allows students access to a large array of online educational resources that we believe can greatly enhance student's learning experience.

The school's **Acceptable Use Policy** is available to be viewed on [www.scoilbhrideb.com](http://www.scoilbhrideb.com) or a paper copy may be requested from the school Secretary.

As the parent or legal guardian of a pupil attending Scoil Bhríde B.N.S. it is advised that you read this policy.

Having read the terms of our school's Acceptable Use Policy, you may like to take a moment to consider how the Internet is used in your own home, and see if there is any way you could make it safer for your own family.

I grant permission for my child or the child in my care, to access the Internet. I understand that the Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by Scoil Bhríde B.N.S to provide for online safety but the school cannot be held responsible if pupils access unsuitable websites.

**I accept** the above paragraph

**I do not accept** the above paragraph

In relation to Scoil Bhríde B.N.S. website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing children's work and photographs on the school website.

**I accept** the above paragraph

**I do not accept** the above paragraph

Parent's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Scoil Bhríde Boys NS**  
**Pupils' Rules for Online Safety**

**Please read and explain the following rules in relation to online safety to your child.**

**1. I am responsible for my own behaviour when accessing the Internet, just as I am anywhere else in the school. I know that normal school rules apply.**

2. I understand that Internet access is a privilege not a right and that using the Internet requires responsibility.
3. I will not use bad language, or send messages that could hurt another person.
4. I must get my teacher's permission to print, or download any text, images, or other data from the Internet.
5. I will never give out any personal information, such as my home address or phone number on the Internet or while using e-mail.
6. I will tell my teacher straight away if I come across any information that makes me uncomfortable.
7. I understand that teachers can read all files and disks used on school computers, including any e-mails I send or receive. Also, I understand that school computers keep a record of what I have viewed on the Internet.
8. I understand that if any of the above rules are broken, then it will result in a temporary or permanent ban on Internet and or computer use.

**I have read, understood and explained in detail to my Child the Pupils' Rules for Online Safety.**

**Child's Name:** \_\_\_\_\_

**Class:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Signature of Parent / Guardian:** \_\_\_\_\_