Acceptable Usage Policy
Scoil Bhride, Kill

Table of Contents

1. *Introduction*

The Acceptable Usage Policy outlines the obligations on all persons who work or deal with Scoil Bhríde and who have access to its information assets.

Users with queries as to how IT systems may be used to support them in carrying out their work or relating to compliance with this policy should record any problems in the LOG BOOK in the office. Users who are unsure about whether an existing set of circumstances or a proposed action is compliant with this policy should contact the principal without delay and before proceeding.

2. *Scope*

All Scoil Bhríde staff and any third parties authorised to access Scoil Bhríde information assets are required to adhere to this policy.

The fundamental principle underlying good practice for information security is that the level of access used by each individual should be set to the minimum required to carry out their responsibilities.

The Acceptable Usage Policy applies to all existing and proposed Scoil Bhríde systems. The Scoil Bhríde reserves and exercises the right to review and audit all documents and data on Scoil Bhríde systems and computer networks.

This policy supersedes all previous policies on acceptable computer use and will be amended annually, every two years or as the Board sees fit.

3. *Enforcement*

Violation of this policy may result in disciplinary action, in the case of others engaged in Scoil Bhríde business, this may result in legal redress. Any person who is aware of or observes a suspected violation of this policy is responsible for reporting the incident to the principal.

4. *Data Classification*

Data owned, used, created or maintained by Scoil Bhríde should be classified accordingly in line with Data Protection policy. In broad terms, below is a table listing suggested data classification categories:

Not Classified/Public	Information available to the general public and approved for distribution outside the Scoil Bhríde
Internal use only	Information not approved for general distribution outside Scoil Bhríde and which does not clearly fit into the other classifications.
Confidential	Includes data covered by the Data Protection Acts under the category of personal data[1]. Confidential also includes information considered to be Management sensitive[2] to Scoil Bhríde, including intellectual property.
Strictly Confidential	Includes data covered by the Data Protection Acts under the category of sensitive personal data[3]

[1] 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. Examples of personal data include a name, address, contact details etc.

[2] Management Sensitive Data relates to any information held by Scoil Bhríde that if disclosed to an unauthorised party could result in, but is not limited to, the loss of public confidence, non-compliance with regulatory requirements, legal liabilities and additional costs. For example, commercially sensitive information may include Psychological Assessments, Occupational Therapist Reports, Procurement interim reports, board papers, contracts, financial reports, budgets or sensitive child specific information.

[3] Sensitive Personal Data relates to specific categories of personal data which include, amongst other criteria, information relating to the physical and mental health of an individual.

5. Ownership and authorised use of Scoil Bhríde information and equipment

All information used or created by Scoil Bhríde either belongs to or is the responsibility of Scoil Bhríde. Access to this information is to be granted on clear business need-to-know basis. Any document, message or correspondence that is created using Scoil Bhríde's resources, whether it is electronic or paper-based, personal or business-related, belongs to Scoil Bhríde. Scoil Bhríde reserves the right to examine all information stored on Scoil Bhríde systems or on Scoil Bhríde computer networks and may perform random audits on a regular basis as required.

All end-user devices (e.g. PCs, laptops, mobile phones, Smartphone devices, web cams, cameras, visualisers, ipads, printers, walkie talkies, video cameras) issued by Scoil Bhríde are the property of Scoil Bhríde.

If any device is defective, it should be reported to the principal/ deputy principal and should not be used if its use might pose a danger or threat to Health and Safety. For example, exposed wires on a lead for a kettle, heater or other. Devices should only be used for their intended use.

6. General Security

You are expected to take reasonable precautions to protect against the unauthorised access or illegal use, disclosure, modification, duplication and/or destruction of any information or technology resource under your control, in accordance with Scoil Bhríde Information Security Policy. The following is a list of "Do's "and "Do Not's" which you should adhere to at all times:

Do's

Do obtain appropriate authorisation for restricted information to which you need access.

Do store information that must not be shared with any other person on your home drive (e.g. H:/ drive).

Do obtain appropriate authorisation from the principal/deputy principal before transmitting confidential or strictly confidential information to a third party.

Do shred or use the confidential waste disposal bins for hardcopies of confidential or strictly confidential information no longer required.

Do use only your assigned User-ID and password, and never someone else's on the photocopier.

Do "shut down" your laptop correctly at the end of the working day when working remotely.

Do ensure all visitors sign in at the reception area.

Do return all Scoil Bhríde devices (e.g. laptops, mobile phones), documents or portable media devices (e.g. USB memory devices, CDs, DVDs) belonging to the Scoil Bhríde upon termination of your employment/contract or on Long term leave, or non-renewal of contract.

Do load only software that has been provided or approved by the Scoil Bhríde and which:

- has a clear educational purpose; and
- has been approved for use by the principal/deputy principal.

Do report any observed or suspected information security weaknesses or incidents to the principal/deputy principal

immediately. Information security incidents may include, but are not limited to, loss or theft of data, laptops or Smartphones, computer virus, unauthorised individual in Scoil Bhríde premises or unauthorised access to data.

Do familiarise yourself and adhere to this AUP.

Do Not's

Do not store or transfer copyright material on the network drives (e.g. H:/, N:/, P:/) or local drives (e.g. C:/) of PCs/laptops.

Do not store confidential or strictly confidential information on your local PC or laptop drives (e.g. C:\).

Do not divulge confidential or strictly confidential information in public network shares, such as NAS.

Do not create/modify any network folders without ensuring that appropriate security is applied to the folder and the content.

Do not copy, alter or destroy confidential or strictly confidential information without appropriate authorisation from the principal/deputy principal.

Do not disclose or discuss any confidential or strictly confidential information to unauthorised individuals both internally or externally.

Do not leave Scoil Bhríde paper documents unattended, such as in vehicles, public areas, meeting rooms.

Do not store Scoil Bhríde owned information on non Scoil Bhríde owned computers.

Do not remove computer equipment, software or information belonging to the Scoil Bhríde from Scoil Bhríde premises without authorisation from your principal/deputy principal.

Do not attempt to connect to Scoil Bhríde computer networks or services with non Scoil Bhríde owned equipment without authorisation from your principal/deputy principal.

Do not use personal owned devices such as portable media players (e.g. iPods), external hard drives or digital cameras in conjunction with Scoil Bhríde computer equipment.

Do not create, execute, forward or introduce any computer code designed to self-replicate, damage or otherwise impede the performance of any computers memory, storage, operating system or software.

Do not uninstall/disable Scoil Bhríde -approved software (e.g. anti-virus) from the system you use.

Do not install or run two anti virus programmes on the same device.

Do not engage in private business ventures using Scoil Bhríde computer systems.

Do not engage in any activity on Scoil Bhríde systems or the Scoil Bhríde computer network that is intended to by-pass information security controls.

Do not allow an unauthorised individual to follow you through an access controlled external or internal door without checking the individual has Scoil Bhríde access authorisation. All visitors must report to the reception area and be accompanied by Scoil Bhríde member of staff while on Scoil Bhríde premises.

7. Loss and theft of Scoil Bhríde devices

The following procedure must be followed in the event of loss or theft of a Scoil Bhríde device.

Event	*Action to Take*
Lost and Stolen laptops, PCs, Smartphone, USB memory keys, or other Scoil Bhríde mobile devices.	1. Notify the principal/deputy principal immediately and inform them of the nature of the information held on the device and whether this includes confidential or strictly confidential information (as defined above).

8. Passwords

Do's

Do keep your passwords confidential at all times and do not share it for any reason. The passwords you choose should be of sufficient strength to deter password guessing or cracking attacks.

Do include numbers, symbols, upper and lowercase letters in your password. The password length you choose should at the very minimum be 8 characters long.

Do change your passwords on a regular basis.

Do provide your computer password to the principal for storage.

Do Not's

Do not choose passwords that are based on repetition, dictionary words, letter or number sequences, usernames, or biographical information (e.g. names, dates, etc).

Do not use incremental passwords (e.g. January1, January2, January3, Password1, 1Password, d1Passwor, rd1Passwo, etc).

Do not write passwords down and under no circumstances leave passwords with your computer equipment.

9. E-mail and Electronic Messaging

Do's

Do remember any document, message or correspondence that is created using the Scoil Bhríde,s resources, whether it is electronic or paper-based, personal or educational-related, belongs to the Scoil Bhríde . The Scoil Bhríde reserves the right to examine all information stored on Scoil Bhríde systems or on Scoil Bhríde computer networks and may perform random audits on a regular basis as required.

Do exercise the same care in preparing e-mails or electronic messages as you would in preparing hard copy documents. Extra care must be taken to ensure that they are complete and correct before being sent.

Do report any received e-mails which you perceive to be obscene or malicious in nature to the principal/deputy principal.

Do save confidential or strictly confidential information, which you have received by e-mail, to appropriate secure storage areas (e.g. nas, databiz).

Do Not's

Do not use e-mail or electronic messaging to engage in any communication that is threatening, discriminatory, profane or can be viewed as harassing or offensive to others based on race, ethnicity, sex, age or otherwise, defamatory slanderous or obscene.

Do not break into the computers or intercept the e-mails and electronic communications of other individuals.

Do not knowingly generate or distribute junk mail or chain letters.

Do not open any e-mail attachments from an outside source that are non-work related during work.

10. Internet Usage

Do's

Do use the Internet lawfully, respectfully, responsibly and as part of the normal execution of your job responsibilities.

Do obey all copyright restrictions if information is obtained from the Internet**.**

Do avoid personal use of the Internet during the hours of 9am – 2:40pm.

Do Not's

Do not download or upload any file, software or utilities, educational or otherwise, from or to the Internet without authorisation from the principal/deputy principal.

Do not attempt to download any file from the Internet where you are not absolutely sure that the source is safe and reliable.

Do not use the Internet to view pornographic, obscene or otherwise offensive material at any time.

Do not use the Internet for gambling or online gaming purposes.

11. PC/Laptop Security

Do's

Do report damage, evidence of interference with equipment or software and the presence of prohibited equipment or software to the principal/deputy principal without delay.

Do carry your laptop in an appropriate case provided when out of the office to avoid any threat of loss or damage.

Do ensure when using a laptop in a public place that the on-screen information is not unwittingly disclosed to unauthorised individuals.

Do Not's

Do not store personal data on laptops.

Do not leave an Scoil Bhríde laptop unattended, such as in a vehicle and public areas.

Do not allow anyone other than you, to use your Scoil Bhríde laptop.

Do not interfere with hardware or software, network connection, connectors, infrastructure or cabling

Do not fit any wireless device or other peripheral or network attachment to a PC or laptop without authorisation from the principal/ deputy principal.

Do not attempt to move, change or upgrade any PC or laptop hardware.

Do not use a PC or laptop where you there is evidence of interference by an unauthorised individual.

12. USB Memory Devices & CD / DVD Writers

Do's

Do lock away all USB memory devices, CDs and DVDs that contain confidential or strictly confidential information at the end of the working day.

Do secure confidential or strictly confidential information on USB memory devices, CDs and DVDs through encryption and password protection mechanisms.

Do ensure that all CDs and DVDs are appropriately destroyed when no longer required.

Do ensure that all information is removed from USB memory devices when no longer required.

Do Not's

Do not use USB memory devices, CDs and DVDs to store Scoil Bhríde confidential or strictly confidential information unless absolutely necessary for educational purposes.

Do not use USB memory devices, CDs and DVDs if you are not authorised to do so by your principal/deputy principal.

13. Print and Photocopy Services Usage

Do's

Do use the PIN security feature for all confidential or strictly confidential prints or photocopies.

Do remove confidential or strictly confidential paper documents from printer or photocopy devices immediately.

Do use printers for Scoil Bhríde related work.

Do report all printer device issues to the principal/deputy principal and enter in the ICT ISSUES BOOK in the office

Do Not's

Do not leave confidential or strictly confidential prints at printer or photocopy devices.

Do not attempt to identify the owners of paper documents left at printer devices by reading the document. Place all paper documents left unattended at a printer device in a secure shredding bin.

Do not use Scoil Bhride photocopier or printer for personal use.

14. Non Scoil Bhride Equipment

Scoil Bhride may provide Internet connectivity on a case by case basis for third parties, such as Consultants, with non-Scoil Bhride laptops or other equipment.

All communications between Scoil Bhride and third party must be accomplished through a controlled secure service appropriate to the data classification of the information being communicated.

15. Monitoring

Scoil Bhride may monitor and intercept electronic communications, whether created for business or personal purposes, at any time. By monitoring the systems, Scoil Bhride is ensuring that its business interests are protected, for quality control purposes, to detect abuse of IT systems and to detect or prevent crime or misconduct.

If you are found to be downloading or sending indecent, obscene, pornographic, sexist, racist or defamatory or other inappropriate materials, as well as the circulation of such materials, you will be subject to disciplinary action up to and including dismissal.

16. Confidentiality

Information relating to the Scoil Bhride or associated organisations must not be revealed other than in the discharge of your duties. Any improper disclosure of information relating to the Scoil Bhride or associated organisations may result in disciplinary action.

17. Compliance with the Data Protection Acts

Scoil Bhride has overall responsibility for ensuring that Scoil Bhride as a whole complies with its obligations under the Data Protection legislation. However, all users who collect and/or control the content and use of personal data are also responsible for compliance with the Data Protection legislation. All users working on behalf of Scoil Bhride who as part of their responsibilities, process personal data, are required to comply with Scoil Bhride Data Protection Policy.

18. Supporting Documents

This policy is supported by the following documents:

a) Data Protection Policy
This document outlines the policy of the Scoil Bhride to meet all of its obligations in respect of the Data Protection Acts.

b) Scoil Bhríde Code of Good Behaviour

This document outlines acceptable behaviour associated with the school.

19. Document Ownership

The owner of this document is the board of management and is responsible for the maintenance of this document.

20. Maintenance

This procedure document will be reviewed and will be amended annually, every two years or as the Board sees fit.Updates to this document will be discussed and reviewed by the staff. This document will be approved by the Board of Management.

Scoil Bhríde Acceptable Usage Policy Pupil Policy

The aim of this Acceptable Use Policy (AUP) is to ensure that pupils will benefit from learning opportunities offered by the school's ICT and Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

It is the policy of Scoil Bhríde to allow our pupils supervised access to the internet for the following purposes:

- As a means of **achieving recognised learning objectives**
- As a means of **communication** between our school and other learning communities
- As a means of communicating information to parents
- As a forum to **display pupils work** and achievements
- To develop **technological fluency** in our pupils

School Strategies

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 follows:

- General Access to internet will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material. The school internet is protected by the firewall provided by the PDST NCTE (National Centre for Technology in Education).
- The school will regularly monitor pupils' Internet usage.
- Pupils and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal USB key fobs or CD-ROMs in school is not allowed.
- Pupils are expected to use the internet in a responsible way as shown to them by their teachers and will not undertake any actions that may bring the school into disrepute. The school cannot be held liable for the improper use of the Internet by pupils.

World Wide Web

- Pupils will use the Internet for educational purposes only.
- Pupils will be familiar with copyright issues relating to online learning.
- Pupils will never disclose or publicise personal information.
- Pupils 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.
- Pupils will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials
- Pupils will be taught appropriate use of the internet, using the www.webwise.ie teaching materials.

Email

- Pupils will not have access to email facilities at school. Any emails to other children / schools, will be sent through the school email address.

Internet Chat (Very restricted use only)

- Pupils will only have access to chat rooms, discussion forums or other electronic communication forums that have been approved by the school (eg. Dissolving Boundaries.
- 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.
- Face-to-face meetings with someone organised via Internet chat is forbidden.

School Website

- Pupils will be given the opportunity to publish projects, artwork or school work on the school website.
- The publication of student work will be co-ordinated by a teacher.
- Pupils' work will appear in an educational context on Web pages.
- The school will endeavour to use photographs, audio or video clips focussing on group activities. Photographs, audio or video clips focussing on individual pupils will not be published without the parents' permission. This permission is inferred unless specifically withdrawn.
- Personal pupil information including surnames, home address and contact details will not be used on school web pages.
- Pupils will continue to own the copyright on any work published.

Personal Devices

The use of mobile phones is prohibited. See the ***Code of Good Behaviour***. Pupils using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera, still or moving is in direct breach of the school's acceptable use policy.

Legislation

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

- Data Protection (Amendment) Act 2003 (see school policy)
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988

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

Sanctions

Misuse of the Internet may result in disciplinary action, including 1) Verbal warning(s) 2) Written warning(s), 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. See ***Code of Good Behaviour***.

Permission Form

The understanding is that all Parents, Guardians and Pupils accept this AUP. We request that in the event of one having any objections or inability to accept this policy, that they print off this page and return to the class teacher or school principal.
Please review the attached school Internet Acceptable Use Policy, sign and return this permission form to the class teacher. This form will be kept on file until your child is finished in Scoil Bhríde.

Name of Pupil: _____Class:_____

Pupil

I agree to follow the school's Acceptable Use Policy on the use of the internet. I will use the Internet in a responsible way and obey the rules explained to me by the school.

Pupil's Signature: _____ Date: _____

Parent/Guardian

As the parent or legal guardian of the above pupil, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school 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** □
(Please tick as appropriate)

In relation to the school 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 on the school website.
I accept the above paragraph □ **I do not accept the above paragraph** □
(Please tick as appropriate)

Signature: _____ Date: _____

Address: _____ Telephone: _____