USE OF POLICY

St. Brigid's
PRESENTATION SECONDARY SCHOOL

ACCEPTABLE TECHNOLOGY (AUP)

ST. BRIGID'S PRESENTATION

SECONDARY SCHOOL

KILLARNEY

CO. KERRY

This policy has been drawn up in consultation with Staff, Parents, Student Council and the Board of Management.   The policy is reviewed regularly.

Before signing, the policy must be read carefully to indicate that the conditions of use are accepted and understood.

Reviewed	Ratified by B.O.M.	Next Review
March 2019	8th April 2019	Academic Year 2020/2021

The aim of this Acceptable Use of Technology Policy (AUP) is to ensure that the school community will benefit from learning opportunities offered by the school's internet and technology resources in a safe, effective manner consistent with General Data Protection Regulations (GDPR). Computer and 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 Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the policy– will be imposed.

It is envisaged that school and parent representatives will review the AUP regularly. Before accepting the schools AUP it should be read carefully to ensure that the conditions of use are accepted and understood.

Introduction

Technology resources at St. Brigid's Presentation Secondary School are provided for the purpose of supporting the educational mission of the school. The school's goal in utilising technology is to promote educational excellence by facilitating resource sharing, innovation, research, creativity, communication, increased productivity and mobile learning.

Use of these technologies is a privilege that carries responsibility and behavioural expectations consistent with all school rules and policies, including but not limited to those stated in the Code of Behaviour. It is understood that members of the school community will use devices and the school's network in a responsible, ethical and legal manner at all times.

The use of the technology resources is a privilege, not a right. The privilege of using the technology resources provided by the school is not transferable or extendible by students to people or groups outside the school and terminates when a student is no longer enrolled in the school.

This policy has been designed to protect the staff, the students and the school. The Board of Management of St. Brigid's Presentation Secondary School, Killarney has a responsibility to support and educate the staff and students in the use of technology to ensure that users do not unwittingly get themselves and the school into an activity that may result in either a criminal action or a legal claim being taken.

The computer network and all individual computers, school laptops, tablets, printers and photocopiers are the property of St. Brigid's Presentation Secondary School, Killarney and are to be used for legitimate school business purposes only. Employees and students ("users") are provided with access to these technologies to assist them in the performances of their work. All users have a responsibility to use the schools' resources, including the internet in a professional, lawful and ethical manner. Use of school owned technologies for private and personal purpose is not permitted, except when authorised by school management through the person of the Principal.

This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the terms and conditions named in this policy, privileges may be terminated, access to the school's technology resources may be denied, and the appropriate disciplinary action shall be applied.

Ratified by the Board of Management Monday 8th April 2019

Violations may result in disciplinary action up to and including suspension for students. When applicable, law enforcement agencies may be involved.

This policy may be updated at any time.

School's Strategy

Staff are required to review this document and abide by the terms and conditions laid out within it.

Students and parents are required to review this document, as well as sign the accompanying agreement to protect the hardware and software inherent with this technology.

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the use of technology including the internet. These strategies are as follows:

General

- Each time users "log on" to the school network they implicitly agree to the AUP of St. Brigid's Presentation Secondary School.
- All users must agree to the AUP of St. Brigid's Presentation Secondary School at "log on" on all machines.
- Users may only "log in" with their own individually assigned Username and Password. The Username and Password may not be shared with anyone within the school community or outside the school community.
- The AUP will be displayed in the Information Technology Room and will be available on the school website.
- Students are not permitted to use technology unless a teacher is present.
- The I.T. room will be locked by the teacher after use.
- Internet sessions 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 will regularly monitor users' technology and internet usage.
- Users 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
- In order to minimise the risk of introducing viruses into the school infrastructure the use of personal discs/flash drives/memory sticks or CD-ROMs in the school requires the permission of the Principal. The school reserves the right to centrally prevent the use of personal discs/flash drives/memory sticks or CD-ROMs.
- Screensavers/Wallpaper or Background are set by the school and may not be altered.
- Users will treat each other with respect at all times and will not undertake any actions that may bring the school into disrepute.

Ratified by the Board of Management Monday 8th April 2019

World Wide Web

- Users will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Users will report accidental accessing of inappropriate materials to the Supervising Teacher/Principal.
- Users will use the internet for educational purposes only.
- Users will be not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement).
- Users will never disclose or publicise personal information
- Downloading materials or images not relevant to their work or studies, is in direct breach of the school's AUP.
- Users will be aware that any usage including distributing or receiving information, school-related or personal, maybe monitored for unusual activity, security and/or network management reasons.

Email

- Users will use their own approved school e-mail accounts only.
- Remember that e-mail is effectively on the school's headed paper and can be traced back to place, date and time of sending.
- Prior to sending an email, users must ensure that they are satisfied with the content and should double check the address of the intended recipient.   Once the "send" key is pressed e-mail cannot be stopped or retrieved.   Deleting mail from your system does not make it untraceable.
- Users will not instigate or forward "junk mail" to users either within or outside the school.
- Users will not make any derogative comment regarding gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of a specific community.
- Users will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
- Users will not reveal their own or other people's personal details, such as addresses, or telephone numbers or pictures.
- From time to time teachers may organise communication with a school abroad either through video calling or via email. Such communication will take place under the supervision of the teacher.
- Students will never arrange a face to face meeting with somebody they met over the internet unless the meeting has been approved by a parent/guardian.
- Should a student receive material, which she finds offensive or abusive or time wasting she should immediately report it to the supervising teacher who in turn will report it to the Principal. Should a staff member receive material, which she/he finds offensive or abusive or time wasting she/he should immediately report it to the Principal.

Internet Chat

- Users shall only have access to chat rooms, discussion forums or other electronic communication forums that have been approved by the school.

Ratified by the Board of Management Monday 8th April 2019

- Chat rooms, discussion forums, and other electronic communication forums shall only be used for educational purposes.
- User names shall be used to avoid disclosure of identity.

School Website

- We aim to give our students an 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 shall appear in an education context on web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Personal student information including home address and contact details will be omitted from school web pages.
- The school will ensure that image files are appropriately named.
- Students will continue to own the copyright on any work published.

Personal Devices

Students are not permitted to use their own technology within the school building or on school grounds without the explicit permission of the supervising teacher. Where a student is found to be using own her technology including a mobile phone or taking still or moving images in the school being or on school grounds are in direct breach of the AUP and of the Code of Behaviour.

Students with Special Educational Needs(SEN):

Technology can be a positive tool for all students and in many cases students with Special Educational Needs can become more independent learners by utilising appropriate technology. St. Brigid's acknowledges and recognises this and therefore students with diagnosed SEN are permitted to use National Council for Special Education (NCSE)sanctioned technologies within the school building. In exceptional circumstances where the technology has not been sanctioned by the NCSE parents/guardians may in writing request permission from the Principal for their daughter to use a specified technology.

Use of Individual Electronic Devices

- Students with SEN who having sought permission in writing from the Principal to use a device in school are responsible for that device. The school cannot be held responsible for the device nor can the school provide any I.T. support for the device.
- Students are required to use the device in a responsible and ethical manner that does not cause disruption to the learning and teaching environment of the class or study hall.
- Students may be selected at random to provide their device for inspection by a staff member i.e. to check homework assignments, to ensure appropriate use of internet etc.
- Students are obliged to be disciplined in the use of the device during class and study. By this it is meant that they will stay 'on task', and not misuse the device for inappropriate activity. 'Off task' use of the device can be defined as the opening or use

of any application not specified by the teacher, going online without the specific instruction of the teacher, and the use of any device functionality not directly related to the lesson or task, or directed by the teacher. Failure to stay 'on task' will invoke the Code of Behaviour.

- The right to use the device can be revoked by the teacher in class, if it is judged that the student is off task.
- Students should carefully follow all the instructions of their teacher in the use of the device. Failure to follow explicit instructions that leads to class disruption will invoke the disciplinary procedure.
- Devices can only be used in class with the permission of the teacher.
- Students are required to obey general school rules concerning behaviour and communication that apply to computer use.
- Students are required to use all technology resources in an appropriate manner so as not to damage school equipment or cause substantial disruption to school life. Substantial disruption can be defined as any outlay of school resources, personnel or material that is a consequence of the disruptive behaviour, including incident investigation, reporting, and repair to damage done. Damage includes, but is not limited to, the loss of data resulting from delays, non-deliveries, or service interruptions caused by the student's own negligence, errors or omissions.
- Students are required help protect our computer system/device by contacting the Principal about any security problems they may encounter.
- Students are required to turn off and secure their device after they have finished working to protect their work and information.
- Students are responsible for ensuring that their device is fully charged at the start of each day and must be allow the cable of their device charger to case a trip hazard when charging their device in school.
- Students are required to print a copy of any email containing inappropriate or abusive language or if the subject matter is questionable, and turn it in to the Principal.
- Students are not allowed to use another student's device without the explicit permission of its owner.
- Private browsing must always be 'Off'.
- Photo, video and audio storage on devices will be for school projects and for personal use. Storage of student personal photos, video and audio or downloaded images, video and audio will be allowed under the parameters given to students by their supervisors. It is expected that all content on the device will be of a moral nature, including photographs. The Principal, IT Technicians, teachers will have the right to inspect the content of the device. Permission must be obtained before taking photographs and recording others and before posting or transmitting pictures or recordings of others.

Activities strictly prohibited when using technology in school:
- Use of a device when explicitly prohibited by a teacher or staff member.
- Illegal installation or transmission of copyrighted materials.
- Any action that violates existing school policy or public law.
- Using a device to photograph, video or record staff or students without their explicit permission.
- Use of chat rooms, sites selling exam papers, book reports and other forms of student work.

Ratified by the Board of Management Monday 8th April 2019

- Use of any Messaging services not authorised by the school e.g. MSN Messenger, ICQ, AIM, IMO, Viber, WhatsApp, Snapchat etc.
- Only approved games, which in no way contradict our mission as a Catholic school, may be used with permission of a teacher.
- Use of outside data disks or external attachments without prior approval from the Principal.
- "Jailbreaking" of your iPad.
- Spamming - Sending mass or inappropriate emails.
- Gaining access to other another individual's account, files, and/or data whether the file has been password protected or not.
- Use of the school's internet/E-mail accounts for financial or commercial gain or for any illegal activity.
- Use of anonymous and/or false communications such as, but not limited to, MSN Messenger, Yahoo Messenger, email, etc.
- Participation in credit card fraud, electronic forgery or other forms of illegal behaviour.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed.
- Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients. Transmission of texts or photographs of an obscene or a vulgar nature.
- Bypassing the web filter through a web proxy or 'anonymous server'.

Student Discipline

The technology, computer, Wi-Fi and server infrastructure are expensive facilities which can only be maintained in good working order with the full cooperation of staff and students. Therefore, intentional, substantial disruption in this area will be taken very seriously. Disruption which requires the deployment of additional resources to resolve may result in a fine for the offending party/parties.

Breaches of the school AUP will be dealt with as per the school's Code of Behaviour.

Legislation

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

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988 to 2018

Signed: _____ Date: _____

Chairperson of the Board of Management

Ratified by the Board of Management Monday 8th April 2019

Ratified by the Board of Management Monday 8th April 2019