Acceptable Usage Policy

Digital Citizenship and Acceptable Information Technology Use

Rationale

Computer and internet resources have become of critical importance to schools in facilitating and supporting learning and teaching. Technology resources are provided to students for educational purposes only.

St Benedict's has established significant ICT resources to support these activities. This document has been developed to inform users of their rights, responsibilities and obligations when using computer and internet resources. These are consistent with Brisbane Catholic Education's requirements that all such resources are used in an ethical, legal and responsible manner.

Objectives

To ensure:

- Our students are taught to use technology in a safe and appropriate manner and follow all rules and requirements when in use.
- Our students understand the importance of confidentiality and cyber safety and are made aware of and are alerted to these dangers.
- Our students respect copyright obligations associated with using this technology.

Implementation of Policy *Responsibilities of Users*

Permitted Use of Technology Resources

Students must only access St Benedict's school technology resources for educational purposes.

Utilising the School Network

When utilising the school computer network students should:

- Use the school's computer network solely for educational purposes within the St Benedict's primary curriculum;
- Obey staff directives and department specific guidelines regarding the use of the St Benedict's primary computer network;
- Use the school computer network in a manner that doesn't cause menace, harassment or offence to others.

When utilising the school computer network students must ensure they do NOT:

- Disclose their username and password details to another person;
- Buy or sell items or services over the internet;
- Access or enter chat rooms, including social media sites;
- Access, post or send inappropriate internet or email content, especially content that is illegal, dangerous, obscene or offensive;
- Amend documents created by another student without that student's consent;
- Disclose other private or confidential information to unauthorised persons;
- Deliberately damage or misuse the computer equipment;
- Gain unauthorised access to any systems by any means;
- Deliberately alter or disrupt the school's computer network;
- Use St Benedict's primary ICT resources to attack or compromise another system or network;

- Download, install or use unauthorised software programs or applications;
- Deliberately install computer viruses or other malicious programs or applications;
- Access or intercept others' electronic communications without permission.

All materials on a student's home drive or external storage devices (such as USB memory sticks, devices, multi-media storage devices, etc.) must be relevant to St Benedict's school curriculum. To ensure this occurs staff may inspect student home drives or storage devices brought onto the St Benedict's school grounds.

St Benedict's uses the Brisbane Catholic Education supplied internet filtering system *Websense Triton Web Security*. This enables the school to allow or block web content and protocols from entering the school network. Any device connected to any of the school networks is filtered through this system. Furthermore, Google Safe Search is enabled as default on all network wide devices.

Students may not connect outside personal ICT devices to the school network or connect to external internet providers while at school.

Copyright must be respected and copyright rules followed. See www.copyright.org.au

Confidentiality and Cyber safety
Social media sites have age restrictions for the protection and safety of young people. Students should be aware that material they post on internet sites (including Facebook, Instagram, Snap Chat and other social media websites) is public. The content of the public posts may have personal implications for students if, for example; potential employers access that material. The content of posts also reflects on St Benedict's and our community as a whole. Once information is on the internet it may not be possible to remove it.

Students should not display personal information about themselves or others in a way which is public. For example; students should not post their own or anyone else's address, telephone number or other personal details on the internet or communicate these details in emails. Students should not distribute someone else's personal information without their permission.

Students should be aware that persons on the internet might not be who they say they are. If they have only met them on the internet, they are strangers and students must not arrange to meet persons who they have met in this way. Students who are aware of situations that seem unsafe are to tell a teacher or a member of leadership.

More information about Internet filtering can be found on the websites of The Office of the eSafety Commissioner at https://esafety.gov.au; Internet Safe Education https://www.internetsafeeducation.com; the Kids Helpline at http://www.kidshelp.com.au; Online Safety via http://www.australia.gov.au/information-and-services/public-safety-and-law/online-safety and Bulling No Way at http://www.bullyingnoway.com.au.

Cyberbullying and Defamation
Students must not use email or the internet to say mean, rude or unkind things about other people or send threatening, harassing or offensive messages. Improper use of technology resources could amount to defamation.

At St Benedict's we have a zero tolerance for cyberbullying. Any actions deemed as such will be dealt with accordingly. Please refer to Infringements.

Security
Students must perform a virus check on all attachments received by email and on all storage devices (e.g.; USB, music devices, etc.) before opening. Students must ask for assistance if they are unsure as to how to perform a virus check or the virus check identifies a problem with the attachment.

Students must select a secure password and keep their username and password information private. Their password should be changed regularly and should be difficult for other people to guess. Students must log off at the end of their computer session. Students must report a suspected breach of security to a teacher or parent.

Copyright
Just because something is on the internet does not mean it is freely available. Copying or downloading material from the internet may be a breach of copyright or other intellectual property rights. Students must not use technology resources to copy, download, store or transmit any such material that may include music files, movies, videos or any other form of media.

Utilising External Internet
When using information technology external to Brisbane Catholic Education and St Benedict's, it is unacceptable for students to associate St Benedict's with sites that would bring its name into disrepute. Examples may include:

- Including the school log onto inappropriate websites;
- Using the school name to identify groups or web pages that condone behaviour contrary to the ethos of Brisbane Catholic Education and St Benedict's;
- Posting photographs on websites that associate the school or its students with unacceptable behaviour;
- Construct or participate in social networking sites that offend, degrade or vilify any member of the St Benedict's community;
- Administer or participate in chat rooms or forums that offend, degrade or vilify any member of the school community.

Infringements

At St Benedict's we follow the **WALK** behaviour education program.

- **W**e Respect
- **A**ct Responsibly
- **L**earn Together
- **K**eep Safe

Failure to adhere to this policy will be dealt with in accordance with the St Benedict's Behaviour Education Policy. The severity of the infringement will be divided into three levels from one to three, with level three being the highest of incident.

Consequences for *Level One Infringements* may include complete or partial loss of access to the computer network for up to two weeks.

Examples of *Level One Infringements* may include:

- Others using your device;
- Installing, deleting, copying or transferring software from a device to other devices without permission;
- Failing to use a device as instructed by teachers during class time;
- Repetitively failing to save and manage own documents;
- Defacing a device with stickers or other markings;
- Using a device before school, lunches and after school without teacher permission;
- Failing to report inappropriate ICT use to teachers or leadership.

In the case of major level two and three infringements students may be suspended or excluded from the school at the discretion of the Principal. Any known breaches of these Acceptable Use conditions must be reported by St Benedict's Catholic Primary School to Brisbane Catholic Education's Legal Counsel and/or Chief Information Officer.

Examples of *Level Two Infringements* may include:

- Repeated level one infringements;
- Removing any identifying barcodes or labels from a device;
- Accessing and storing inappropriate or non-school based images, text, audio and video on a device/device;
- Being disrespectful to others on electronic communication;
- Posting images and messages on social media;
- Posting inappropriate images or content to any digital space
- Accessing or intercepting others' electronic communications without permission.

Examples of *Level Three Infringements* may include:

- Repeated level two infringements;
- Wilfully damaging school ICT property;
- Cyberbullying;
- Malicious intent to disrupt the school network;
- Deliberately installing viruses or other malicious programs;
- Hacking any school services not deemed for student use;
- Bringing St Benedict's Primary School name into disrepute by inappropriate use of the school logo or school name.

In the case of major infringements students' inappropriate ICT use will be reported to the local police at the Principal's discretion.

Please read this document carefully. Each student and his/her parent/legal guardian must sign the acknowledgement to confirm that they understand the requirements of our *Acceptable Usage Policy* and the potential consequences of a breach of this policy.

In adherence with this policy the following additional documents will need to be read, understood and signed:

1. *Digital Citizenship Agreement.*
2. *1 to 1 Device Program: Student and Parent Agreement*