St Brigid's Catholic School
New Norfolk

POLICY ON ACCEPTABLE USE OF ICTs

RATIONALE

Information and communication technologies are becoming increasingly vital for effective teaching and learning in a modern-day context. ICT can significantly enhance student learning and provide them easy access to the wider world. There are, however, potential dangers using ICT that we must plan for and guard against as part of our duty of care.

1. INTRODUCTION

Information and Communication Technologies (ICTs) are provided for staff and students of the school to:

- enhance learning opportunities
- promote learning achievement
- support the professional work of staff in the school
- enhance the school's administrative and management of information.

St. Brigid's Catholic School has a duty of care toward both students and staff and, consequently, the use of ICTs within the school by students and staff needs to be responsible, legal, appropriate and for educational purposes. In addition, the use of ICTs needs to be consistent with the aims, values and objectives of the school.

Staff and students of the school are expected to follow the guidelines which are provided to achieve such use.

This policy applies to the use of all school related ICTs for educational purposes, regardless of whether the ICTs are provided by the school or a student.

Both students and their parents or guardians must read this policy (which is available on the school website). The school will provide a copy of the Letter of Agreement which must be signed at point of entry into the school. (see 2014 ICT agreement gr3-6 or Kinder to Gr 2)

The ICT Coordinator will provide a copy of the Letter of Agreement for all existing students at the school each year.

Access to the ICT resources will be provided after a signed Letter of Agreement is returned to the school and for so long as the student abides by the agreement.

2.   DEFINITIONS

2.1   For the purpose of this policy, Information and Communications Technologies (ICTs) are defined as being any electronic device or application which allow a user to access, receive, record or send information, as text, images, audio or video.

2.2   ICTs include but are not restricted to:
- Computer systems and applications such as email and the Internet
- Mobile devices such as mobile phones, iPads and other tablet devices and PDAs
- Web-based tools such as social networking sites, chat rooms, blogs, podcasts, and instant messaging systems
- Imaging tools such as video, still or web cameras and related software
- Audio tools such as audio recording devices, iPods and mp3 players and related software
- Fax and copying machines

3.   ACCEPTABLE USES OF ICTs

Students are expected to do three things in their use of ICTs at school:
- Keep themselves safe
- Respect others, and
- Respect the school's resources.

To achieve these aims, students are expected to do the following things:

3.1   Keeping safe

To achieve this, students will:
- Keep passwords and personal work secure

- Only use the internet and email for educational purposes
- Always seek teacher advice and permission before providing personal details online
- Always obtain teacher permission before publishing any personal information or photos on the school network or online

3.2   Respect others

To achieve this, students will:

- Respect the rights, beliefs and viewpoints of others
- Follow the same standards of behaviour online as they are expected to follow in real life
- Follow the Netiquette guidelines (listed at the end of this document) for online communications
- Respect the ideas and artistic works of others by observing copyright rules
- Acknowledge the author or publisher of information from the Internet and do not claim the work or pictures of others as their own

3.3   Respect resources

To achieve this, students will:

- Use ICT equipment and resources with in the school for educational purposes under teacher supervision
- Follow teacher directions for accessing files, programs, email and Internet resources
- Seek advice from a teacher before responding to unfamiliar online prompts
- Delete emails from unknown sources without opening any attachments (they may contain a virus)

4. UNACCEPTABLE USES

The following uses of ICTs are unacceptable at St. Brigid's Catholic School.

4.1   Personal safety

Disclosure of personal information to strangers or unknown recipients can expose a user to a variety of dangers. These dangers may include such things as exposure to physical danger, inappropriate material, unsolicited commercial material, financial risks, harassment and bullying, exploitation, unreliable information, nuisance and sabotage.

Students will **NOT**:

- Send or post detailed personal information, images or audio about themselves or other people. Personal information includes personal contact information such as home address, telephone or mobile number, school address, work address, email addresses, etc.
- Meet with someone a student has met online without their parent's/guardian/s approval and participation.
- Accept as a friend on social networking sites someone a student does not know.

4.2 Illegal activities

Students need to be aware that they are subject to saws relating to the use of ICTs.

The school can and does log network use. An approved electronic audit of such logs may be provided to police as part of legal investigations.

Students will **NOT**:

- Attempt to gain access to any computer system or service to which they do not have authorised access. This includes attempting to log in using another grade's or person's account or accessing another person's files or emails.
- Make deliberate attempts to disrupt other people's use of ICTs.
- Make deliberate attempts to destroy data by hacking, spreading computer viruses or by any other means.
- Engage in any illegal act, such as threatening the personal safety of others, arranging for a drug sale or the purchase of alcohol, engaging in criminal activity etc.
- Install or use software that is not licensed by the school, without express teacher permission .

4.3 Network security

Students should **NOT**:

- Provide passwords to another person or in response to a request via email (even if the email looks like it comes from someone they know).
- Go looking for network security problems, because this may be seen as an attempt to gain unauthorised access to the network.

- Post information that, if acted upon, could cause damage to or disrupt the network.
- Open emails from unknown sources.

4.4 Inappropriate language

Restrictions against 'inappropriate language' apply to public messages, private messages, and material posted on web pages.

Messages sent using the school's ICTs may be monitored or scanned.

Students should **NOT**:

- Use obscene, profane, rude, threatening, sexist, racist, disrespectful or inappropriate language.

4.5 Respect for privacy

Students should **NOT**:

- Repost messages that were sent to them privately without permission of the person who sent the message.
- Take photos, sound or video recordings of people, including background figures and voices, without their permission
- Distribute private information, including photos and recordings, about another person without their permission

4.6 Respect for others

Students will **NOT**:

- Make personal attacks on another person
- Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If someone tells you to stop sending them messages, you must comply with their request.
- Send or post any inappropriate or inaccurate information, comments, images, video or audio about other people or organisations.
- Send or post personal information about other people without their permission.

4.7 Respecting resource limits

Students should **NOT**:

- Use ICTs for other than educational activities unless given permission to do so by a staff member.
- Download or send large files (greater than 5Mb) without teacher permission.
- Post or respond to chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.

4.8 Plagiarism and copyright

Students should **NOT**:

- Plagiarise works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they are your ideas or writing.
- Use material from the Internet in any manner that violates Australian copyright laws.
- Access or use material from the Internet that relates to exam cheating or providing completed assignments.

4.9 Access to inappropriate material

Attempts to access inappropriate material using the schools ICTs is monitored and logged by the school.

Some inappropriate material is filtered or blocked by the school.

Students should **NOT**:

- Access material which is not relevant to their education
- Use ICTs to access material that:
    - is profane or obscene (pornography)
    - advocates illegal acts
    - advocates violence or discrimination towards other people
    - could be considered rude or offensive by others
- Participate in online chats, discussion groups or mailing lists that are not relevant to their education.
- Use the school ICTs to purchase, order or sell any goods. A special exemption may be made if the purpose of such access is to conduct educational research and both the teacher and the parent/guardian approve access.

5.   NOTIFICATION

Students **WILL**:

- Disclose to their teacher any messages they receive that are inappropriate or disturbing.
- Notify the ICT Coordinator if they identify a possibly security problem.
- Immediately disclose accidental access to inappropriate material to the ICT Coordinator. This will protect students against an allegation that they have intentionally violated this Acceptable Use of ICTs Policy.
- Notify their teacher and/or the ICT Coordinator if they are offended by another person's use of ICTs.

6.   CONSEQUENCES OF IMPROPER USE

Any user violation will be recorded and may be subject to the following consequences:

- Loss of access privileges for a period of time
- School detention
- Informing of parents/guardians
- Legal action

7.   NETIQUETTE

Netiquette refers to guidelines and etiquette for online communication.

Students should:

- Ensure that their email and online messages are written carefully and politely. They should also try to keep messages short and precise.
- Check their email regularly and delete unwanted messages promptly.
- Use appropriate language. Assume that everything posted online is public.
- Be cautious in their use of humour and satire. Sometimes what one person considers funny can be misinterpreted by others.
- Respect the rights, beliefs and viewpoints of others. Every person has a right to this.
- Follow the same standards of behaviour online as they are expected to follow in real life.
- Ensure Caps Lock is off when typing text, as typing in all capitals online is the equivalent to shouting.

This policy and associated practices will be reviewed as part of the St Brigid's Catholic School policy review cycle.

Implemented
Reviewed and amended July 2013