DIGITAL DEVICES POLICY

School Board Policy Number Six
School Board Policy Number: Six

Endorsed: __________________________

Review: ____________________________

Signed: ____________________________
(Chairperson)

Signed: ____________________________
(Principal)
St Brigid’s Catholic School ~ School Board Policy Number Six

DIGITAL DEVICES

Philosophical Basis

Education Purpose
St Brigid’s Catholic School has a duty of care to ensure the safety of all students and staff. This involves the provision of a safe physical and emotional environment for students and staff.

St Brigid’s Catholic School provides staff and students with access to an electronic communications system that enables internet and intranet (internal) access. With the rapid development in electronic communications these communications are having many profound effects on society.

The purpose of Internet use at St Brigid’s is to:
- raise the educational standards
- promote student achievement
- support the professional work of staff
- enhance the school’s management functions

Internet use is part of the curriculum and is a necessary tool for learning. Internet access is an entitlement for all students who show a responsible and mature approach to its use. The Internet is an essential element in 21st Century life for education, business and social interaction. Generally students use the Internet widely outside the school and will need to learn how to evaluate Internet information and to take care of their own safety.

St Brigid’s Catholic School Internet access is designed expressly for student use and has age appropriate filtering through the CEO SINA system. All students will be taught what Internet use is acceptable and what is not. Internet access will be planned to enrich and extend learning activities. Students will be educated in the effective use of the Internet in research activities.

St Brigid’s Catholic School must be concerned about the safety of their students when they have access to Internet and Network Services. St Brigid’s Internet is not a public access service or a public forum. St Brigid’s has the right to place reasonable restrictions on the material students and staff access or post through the system. Users are expected to follow the rules set forth in this policy and the law in the use of the Internet at St Brigid’s.

Servers will be located securely and physical access will be restricted. The server operating system must be secured and kept up to date. Future access by wireless devices must be pro-active and security encrypted.

Users may not use the service for political lobbying. Staff and students may use the service to communicate with their elected representatives and to express their opinion on political issues.

This policy covers all digital and electronic devices that children bring to school including but not exclusively, electronic games, MP3 Players (eg Ipods), USB/flashdrives (non school supplied), digital cameras and mobile phones.

Mandatory Provisions

Our school does not allow digital and electronic devices to be brought to school as they are valuable and may be lost, stolen, broken and they can be disruptive to teaching and learning.

However, we recognise that some students require Access to a mobile phone for safety reasons when coming to school and from school.

The possession and use of digital and electronic devices presents a number of challenges for the school, including:
- Digital and electronic devices can be valuable items and might render a student vulnerable to theft or the item being broken.
- Digital and electronic devices can make pupils objects of envy and could have implications with regard to discipline and potential bullying.

Social Networking and Class Web pages
St Brigid’s will block the access to social networking sites. Newsgroups will be blocked unless a specific use is provided. Students will be taught about the importance of never giving out personal information or photographs.

Teacher’s blogs or wikis need to be password protected. Any class webpage needs to follow the same expectations as that of the school wide website. Parental permission must be received to put up any photos on such pages.

Filtering
Maintenance of the filtering system will be the responsibility of the Principal, eLearning Coordinator and the IT Technician. This is a major task and must be reviewed regularly. A regular check of school internet access must be carried out and a review of popular sites visited and internet search carried out via a search engines.
Responsibilities
The school cannot be responsible for direct supervision of every student while they are using the Internet and Network services and this fact must be made clear to parents. However, reasonable precautions to minimize this danger would include personal safety strategies such as protective behaviours training or appropriate decision-making skills and the provision of personal safety information to the parents. Additional activities could include personal safety instruction for the students and personal safety posters placed by the school computers. Filtering tools are installed to protect students from accessing inappropriate material or receiving offensive emails. In addition, the administration tool (SINA), aids in the supervision and tracking of internet usage. Staff should also be instructed about personal safety issues and the behaviours that students might exhibit when they may be involved with a stalker.

The responsibility of the Principal will be to ensure that all staff are familiar with this policy and establishing a process to ensure adequate supervision of students using the services. The responsibility of parents will be to address with their children any additional boundaries of what is considered acceptable use by members of their family.

Student Internet Access
The Web is a global system providing access to information from around the world. Students may have access to Internet Web information resources through their classroom, the Resource Centre, or the school’s information Technology Centre.

Email is an electronic mail system, which allows students to communicate one-to-one with people throughout the world. Students may have email access only under their teacher’s direct supervision using a classroom account. Student access will be provided on the signing of an “Acceptable Use Agreement” by the parents and the students beyond Year 3. Where possible, computer monitors will be placed in a visible location where both students and staff can discourage attempts to use the system inappropriately.

All users are able to connect to the Internet from any workstation within the school, the ICT lab, classrooms, Resource Centre, teacher preparation room etc.

Through our Local Area Network (LAN), each user accesses the internet through the Catholic Schools Virtual Private Network (VPN), which utilizes an individual user name and password to monitor, record and filter access. Through the VPN all users access email that is also filtered. Each user has an individual email account.

Individual users are responsible for the security of their information through individual passwords. They must take all reasonable precautions to prevent others being able to use their accounts.

Group accounts: accounts can be established for Junior Primary classes to log onto the system. For a particular activity of a class (or group) can have a group internet account set up for a period of no more than one term. The responsible teacher will be given monitoring privileges which they will need to review regularly to ensure the account is being used appropriately.

Parents will be made aware through the school newsletter of the Internet and email access available to students and asked to write to the school if they request their child not to have the level of access normally provided. Where parents have not notified the school of limited access for students then full access will be available.

Unacceptable Uses
You will not post personal contact information about yourself. Personal contact information includes your address, telephone, school address, work address, etc. This information may not be provided to an individual, organization, or company, including web sites that solicit personal information. You will not agree to meet with someone you have met online without your parent’s approval. Your parent should accompany you to this meeting. You will promptly disclose to your teacher or other school employee any message you received that is inappropriate or makes you feel uncomfortable.

Personal Security
Users are not to attempt to gain unauthorized access to the service or to any other computer system through the service, or go beyond their authorized access. This includes attempting to log in through another person’s account or access another person’s file. You will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. You will not use the St Brigid’s network to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, threatening the safety of person, etc.
Network Security
Personal passwords are not to be provided to another person for accessing services. Users are to notify the school network administrator if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an unauthorized attempt to gain access. Users are not to spread computer viruses.

Basis of Discretion
Whilst recognising that mobile phones are an aid to safety and security for some children they too are a cause of concern. For example:
- Even when apparently silent, the use of mobile phones for any purposes could potentially undermine classroom discipline.
- The use of a mobile phone with an integrated camera or video could lead to child protection and data protection issues with regard to inappropriate capture, use or distribution of images. Should the student need access to a camera for school purposes the school will supply the camera.

Some students require access to a mobile phone for safety reasons when coming to school and from school, they may bring them to school subject to the following condition:

The parent/carer should inform the school by completing the form in Appendix A.

Guidelines for the usage of Mobile Phones:
- Mobile phones are not to be used for any purpose on school premises, grounds or during off-site activities e.g. camps and excursions.
- Children are to sign in their mobile phone to the Front Office for safe keeping as they arrive at school and sign their phone out at the end of the day.
- Parents and carers can contact children if required by leaving a message with the school secretary.
- If children require the use of a phone in an emergency they should request the use of the phone at the front office.

Consequence of children bringing digital and electronic devices to school:
- Where a student is found to have a digital or an electronic device it will be confiscated and a parent/carer will be contacted by phone and asked to collect the device from school.

Inappropriate Language
Restrictions apply against:
- The use of ‘Inappropriate Language’ in public messages, private messages and material posted on Web pages
- The use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- Posting information that, if acted upon, could cause damage or a danger of disruption.
- Engaging in personal attacks, including prejudicial or discriminatory attacks.
- Harassing another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.
- Knowingly or recklessly posting false or defamatory information about a person or organization.

Respect for Privacy
Restrictions apply against the:
- The re-posting of a message that was sent to them privately without permission of the person who sent them the message.
- Posting of private information about another person.

Respecting Resource Limits
Restrictions apply against the:
- Use of the services for other than educational and professional or career development activities.
- Downloading or sending of large files (>1Mb) unless approved by IT staff or Administration.
- Posting of chain letters or engaging in “spamming”. Spamming is sending an annoying or unnecessary message to a large number of people.
- Not checking e-mail frequently, deleting unwanted messages promptly.

Investigation of Inappropriate/Illegal Activities
Service users have a limited privacy expectation in the contents of their personal files. In the routine maintenance and monitoring of the network, discovery of an infringement of this Policy or the law may be found.
In which case an individual search will be conducted, with the approval of the Principal, if there is reasonable suspicion that a user has violated the law. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation.

In the event there is an allegation that a student has infringed the intent of the school’s Acceptable Use Agreement, the student will be provided with notice of the alleged violation and an opportunity to present an explanation before a neutral administrator.

Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. This would ordinarily be based on the implementation of the school’s Behaviour Management and Personal Responsibility Policy or could involve the removal of the privilege of internet access.

Staff infringements of this policy will be handled in accord with CEO policies and guidelines. Staff should be aware that their personal files may be discoverable during routine maintenance. St Brigid’s School will cooperate fully with Local, State, or Commonwealth investigators in any investigation concerning to or relating to any illegal activities conducted through the service.

Respecting Others Work
Restrictions apply against:
- Plagiarising works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- Not respecting the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

Internet Safety
Each year the school will facilitate an Internet Safety program for all students across the school. These sessions will occur at the beginning of Term One (prior to the end of Week Four) and another will occur at the start of Term Three (prior to the end of Week Four). Every odd year the Middle School students will participate in a series of e-Safety workshops which reflect the needs of that group.

Emergent technologies
Many emerging technologies offer the potential to develop new teaching and learning tools. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Mobile phones will not be used during lessons or formal school time. Digital cameras can be accessed within the school. Students are not to bring personal digital cameras into school. Digital cameras are not to be taken into any private areas within the school (for example toilets, changing areas etc.). Students must be made aware that their image is being captured.

Cyber bullying
St. Brigid’s school is aware of the issue of cyber bullying and actively facilitates student learning about cyber bullying. Any incidents of cyber bullying will be handled in accordance to the eSafety complaints statement below.

Handling e-Safety Complaints
Complaints of Internet or eLearning misuse will be dealt with by a member of the leadership team. Any complaint about staff misuse will be referred to the leadership team also. Students involved in these complaints will have their parents or caregivers informed. Parents, students and the school will need to work in partnership to resolve the issues.

As a general rule the following consequences will apply:

<table>
<thead>
<tr>
<th>Occurrence</th>
<th>Procedure</th>
<th>Parental Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>Student will lose usage of internet and email privileges for a period of 3 weeks</td>
<td>Parents informed via letter</td>
</tr>
<tr>
<td>2nd</td>
<td>Student will lose usage of internet and email privileges for a period of 6 weeks</td>
<td>Parents contacted via phone and follow up letter</td>
</tr>
<tr>
<td>3rd</td>
<td>After a consultation between leadership, parents and student the student will lose all computer privileges for a period of 1 term</td>
<td>Parent Meeting</td>
</tr>
</tbody>
</table>

Any further occurrences will be dealt with in consultation between leadership, parents and student.
APPENDIX 1

Intranet Permission Letter

Attached is an abbreviated copy of our school’s draft Internet Acceptable Use Policy and Agreement. The Internet offers a range of experiences that can enhance learning, such as researching online museums and libraries, and communicating with others and publishing students’ work.

As with other areas of life, such as television viewing and reading magazines, there are some parts of the Internet that are not appropriate for children. We have several strategies planned to ensure that students are able to use this technology in a positive and appropriate way.

Supervision
Internet will only be accessed within the classroom, Resource Centre or other rooms if there is a staff member or adult to provide supervision.

Content
Content will be screened automatically as we are accessing the Internet through the catholic.edu.au facility. This service blocks access to a range of inappropriate sites.

Security
Passwords will be required to log onto the Internet. Whenever a user logs on, our software records what sites have been accessed, if attempts have been made to access blocked sites and who has made the attempts.

Making expectations clear
It is important that all students are aware of what behaviour and content is acceptable when using this technology.

Staff would appreciate you taking the time to read this policy with your child/ren to help them develop an understanding of what behaviour and content is acceptable. We realize that there are some areas of the policy that may be difficult for some students to understand at this time, either because of their age or because they are not familiar with the Internet.

At school we have explained the relevant sections to students in language appropriate to their understanding. This has varied from class to class, depending upon the age of students. Across all levels, we will relate it to being similar to going to a video store: some videos are great for children, some are meant for teenagers and others for adults.

The Internet differs however, in that the sites do not come with ratings, so students will need to use their judgement to select appropriate sites. If a student comes across a site that made them feel uncomfortable or is inappropriate for them, perhaps because it is too violent, then we want them to tell their teacher.

Students will be receiving instructions in the use of the Internet at a level appropriate to the student’s class, including the skills that will enable them to follow the guidelines set out for school Internet use.

Assistance for younger students
Because of the reading and writing skills required to access the Internet, it is likely that Junior Primary students will need the assistance of an adult or an Upper Primary student to help them.

Student agreement
This is included in the policy as a means of encouraging responsible use. Our intention is that students demonstrate their intention to use this privilege responsibly. If you feel that your child is too young to understand this, but you would still like them to access this technology, then we will accept you signing the parent agreement only.

Photos
Students would remain anonymous if their photos are published on the Internet.

Students would remain anonymous if their photos are published on the Internet.

Please complete and sign the attached Internet/Intranet Use Agreement and return to the office.

Please feel free to make enquiries at school if you require further information.
When using the Internet, email or other online activities:

Students will:
- Always ask permission from the teacher before accessing the Internet.
- Only use the Internet to look for suitable material. As a guide, this means G rated material or PG material with the permission of a staff member.
- Tell a staff member immediately if inappropriate information has been accessed. This will protect students against claims of intentional violation of this policy.
- Keep their passwords secret, and tell a staff member immediately if they believe someone else is using their account.
- Use appropriate manners and language at all times (i.e. within emails and when chatting to others).

Students will not:
- Use the Internet without permission.
- Access inappropriate material. This includes images or messages that are rude, encourage illegal acts, violence or discrimination towards others or are offensive to others.
- Tell others their own password.
- Give out personal information about themselves or others (e.g. names, addresses, phone numbers etc.).
- Enter a chat site without permission from a staff member.
- Log onto the network using another person’s account or password.
- Reuse a school disk that has been used at home without scanning it for viruses.
- Change any computer settings without permission from a staff member.
- Install software onto computers without permission from a staff member.
- Download large files without permission from a staff member. (This can slow down the whole school’s Internet use at times).
- Use the computers to engage in any illegal activity (e.g. copying software).
- Send messages that may offend a person or group of people.
- Copy work from the Internet and claim it as their own.

Student Section

Student’s Name: ______________________
Date: ________________________________

I have read or had explained to me and I understand the Internet/Intranet Use Agreement. I agree to follow the rules and be a responsible user of this privilege. I understand that if I break the rules I may be banned from using this privilege or face other appropriate consequences.

Student’s signature: ____________________
Date: ________________________________

Parent/Guardian Section

I have read St Brigid’s Catholic School Internet/Intranet Abbreviated Policy and have discussed the content with my child. I agree to the terms listed.

I give St Brigid’s Catholic School permission to provide Internet and email access for my child.

Parent’s signature: ____________________
Date: ________________________________
APPENDIX 2

Mobile Phone Parent/Carer consent Form

Mobile Phone
Some students require access to a mobile phone for safety reasons when coming to school and from school, they may bring them to school subject to the following conditions:

- Mobile phones are not to be used for any purpose on school premises or school activities e.g. camps and excursions.
- Children are to sign in their mobile phone to the Front Office for safe keeping as they arrive at school and sign their phone out at the end of the day.
- Parents and carers can contact children by leaving a message with the school secretary.
- If children, in an emergency, require the use of a phone they should request the use of a phone at the front office.
- Students found in possession of mobile phone between 9.00am and 3.15pm will have it confiscated immediately. The mobile phone will only be returned to a parent or guardian.

My child requires their mobile phone in case the need arises when coming to school and from school.

I have read the Digital Device Policy + Appendix 1 & 2 and understand the conditions regarding the use of mobile phones at school.

Child’s Name: ________________________________

Class: ________________________________

Parent/Carer’s Name: ________________________________

Signed: ________________________________

Date: ________________________________

Please return to your class teacher in a sealed envelope marked: Internet/Intranet Use Agreement/Mobile Phone Consent Form

Resources

This policy will be guided by the Information Communication Technology committee at St Brigid’s Catholic School and ICT Support team from Catholic Education S.A.

Evaluation

It is expected that the Digital Devices Policy will be reviewed on a regular basis.

It is anticipated that this will occur every 2 years.