Communication Technology Policy

Rationale

Bayview College acknowledges that the Internet and Information communication technologies (ICT) play an increasingly important role in the learning of young people and the creation and delivery of content by teaching staff. Our Mission statement states that Bayview will assist students "to develop their strengths by providing them with the tools necessary to do so" consequently we are compelled to keep abreast of the technological changes that are occurring. This Communication Technologies Policy applies to all users of the School Network and School owned or leased equipment.

Policy Statement

To ensure all staff and students of Bayview are accessing and using communication technologies in an acceptable manner in accordance with our Student Code of Conduct, Bayview Employment Agreement, policies and the law.

- To communicate the acceptable use of communication technologies to staff and students.
- To communicate an individual's rights and responsibilities when using communication technologies.
- To ensure that all users take appropriate precautions when using communication technologies including the protection of passwords and safe transport and storage of equipment.
- To ensure the security of data on the Bayview network or another technological device.
- To promote appropriate and lawful use of data copying, use and distribution.
- To ensure that School communication technologies are **not** used to facilitate behaviour which is either inappropriate or illegal.

Bayview believes that the benefits for students and staff of being able to access communication technologies far exceed any inherent disadvantages. These benefits include access to global and up to date information resources, opportunities for collaboration, both within the School and with the wider community, and personalised learning.

The establishment and implementation of an acceptable use policy, guidelines, resources and user agreements for students/parents/caregivers, and administrative/teaching staff:

- Contributes to the provision of a safe learning environment and addresses the emotional, physical and social development of young people;
- Contributes to the maintenance of a safe working environment and;
- Assists Bayview to meet its obligations and deliver a curriculum in a manner that is consistent with the Schools vision, mission and values.

The Communication Technologies Policy provides staff and students with the opportunity to utilise these technologies appropriately to enhance teaching and learning in a safe physical and emotional environment.

For the purpose of this policy, communication technologies include, but are not limited to:

- Computers and the School network
- Internet
- Mobile phones
- Wireless Devices
- Personal music devices including MP3 players
- PDAs
- Recording devices
- Portable storage, including USB and flash memory devices

The use of the Bayview computer network, internet access facilities, computers and other technological devices on or off the School site should be for educational or professional purposes. The use of privately owned technological devices or equipment on the School site or at any school related activity must be appropriate to the school environment and in accordance with the guidelines of this policy.

It is an expectation that staff and students will make responsible use of communication technologies at all times. When using global information systems such as the Internet, every attempt will be made by the School to filter out any inappropriate material.

Procedures for Implementation

RIGHTS AND RESPONSIBILITIES

Each staff member and student is held responsible for his or her actions when using communication technologies. Inappropriate use will be dealt with according to the Student Code of Conduct or Employment Agreement. Examples of such unacceptable use include any conduct that:

- Violates or infringes the rights of another person, including their right to privacy
- Initiates access to inappropriate or illegal material
- Initiates access to material which contains real or potentially defamatory material, false, inaccurate, abusive, obscene, violent, pornographic, profane, sexually-explicit, sexually-oriented, threatening, racially offensive or otherwise biased discriminatory or illegal or any other inappropriate material
- Violates copyright
- Violates any other school policy. (e.g. Harassment Policy)
- Broadcasts unsolicited personal views on any matter
- Places images, text or audio-visual content of a member of the school community on the school network or any global information system (e.g. social networking sites)without express permission
- Fails to use the system as prescribed thus permitting infection by computer virus or deliberate infection by computer virus.
- Results in unauthorised external access to the school's electronic communication system.
- Results in unauthorised distribution of BAYVIEW course materials to a third party.
- Involves the unauthorised installation and/or downloading of non-school endorsed software.
- Involves unauthorised repairs.
- Offends or potentially offends the reputation of the school.

In the event of accidental access of such material, users should:

- Not show others.
- Close or minimise the window.
- Report the incident immediately to an appropriate person.

DEFINITIONS:

Acceptable use refers to common sense, decency and legal responsibilities applied to the Network and the writing of emails, messaging, documents, use of a camera facility and downloadable audio and video footage. Users must accept that at Bayview communication technology's primary use is for educational and professional purposes.

Communication Technology Policy Agreement refers to the agreement that Bayview students and staff sign when they enter the School. It refers to the Communication Technology Policy and indicates an agreement to abide by the policy. See Appendix 1.

Downloads refers to the downloading of software from the Internet or the downloading of audio or visual material from web pages (this occurs every time you enter the Internet),mobile phones and other devices.

Email refers to all technologies used to transfer electronic messages, including email from one computer to another; instant messaging, SMS and peer-to-peer file exchange.

Internet means the worldwide communication system of interconnected networks and computers which connects people through their computers. The computers communicate using a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol).
Netware Directory Service refers to the network system used by Bayview

Network Administrator means the person/s appointed by the Principal to manage and supervise the Network. The Network Administrator has been delegated special rights of access and control that are not available to other users and which are intended to be used to guarantee the security of the Network.

Network means the School's computer network which includes access to the **intranet** of the School, the global Worldwide Web through the Internet, email, software, file/data information and hardware.

Unacceptable use refers to any use that:
• violates the values and policies of the School
• violates the law (including the Privacy Act 2000)

User means a person authorised to use the Network.

THE SCHOOL COMPUTER NETWORK

The contents of the Bayview network (including email) remain the property of Bayview.

NETWORK PASSWORDS

   • Users are advised to make network passwords a combination of numbers and letters; these should be a minimum of 8 characters in length with a combination of upper case and lower case.
   • Users should endeavour to keep their passwords confidential at all times.
   • Users are advised to not disclose passwords to any other person.
   • Users are not permitted to share passwords in order to use school network facilities.
   • If a User suspects that someone else is aware of his/her network password, they can alter their network password.

COMPUTER NETWORK USE

   • The use of the network should be consistent with the vision, mission, values and policies of the School.
   • Network accounts should be used only by the authorised user.
   • Software should not be installed or copied from the School network without first checking with the Network Administrator. This is to ensure that the School has the legal license to the software and the user and the School are complying with copyright law.
   • The privacy of information is valued by the School. To enhance this, staff and students are issued with their own personal folder on the 'P' drive to save their information and files to. This drive is only accessible by the user when they have logged in to the network. This drive should be organised and managed efficiently by the user.
   • Archival material from the Personal Folder should be burnt to CD or DVD or an external storage device and deleted from the Network periodically (i.e. each semester).
   • A Staff Shared Folder is available for staff to save information to for all staff to access. Archival material should be burnt to CD or DVD and deleted from the Network periodically (i.e. each semester).

USE OF EMAIL

Email is a major means of formal communication between staff, students, parents and the wider community. It is expected that all BAYVIEW users of email follow the protocols set out below.

EMAIL PASSWORDS

   • Email passwords should follow the same guidelines as network passwords.
   • If a User suspects that someone else is aware of his/her email password, they should alter their email password.

EMAIL USE
   • The use of email should be consistent with the vision, mission, values and policies of the School.
   • Users are encouraged at all times to exercise great care when creating email messages. Appropriate/acceptable language, data and pictures should be used with care and consideration in email messages.

• The intended audience of the email needs to be kept in mind when constructing the content of the email to ensure the appropriate level of formality or informality and structure of the document. External emails should comply with the Bayview Style Guide.
• Users are encouraged to not reveal personal details or information in an email as this can be easily forwarded to recipients they don't know and therefore, email is inherently not secure.
• Users should ensure that messages are addressed to the appropriate recipient.
• Users should not use email in an unacceptable manner as defined by this document in Definitions.
• Emails emanating from Staff will contain the following notice to advise the receiver of potentially confidential or sensitive material:

This message contains confidential information intended for the use only of the addressee named above. If you are not the intended recipient of this message you are notified that you must not disseminate, copy or take any action in relation to it. If you have received this message in error, please immediately notify the sender

• Users must be aware that email messages which they send may be construed as representing the School's position. Where a User does not have the authority, is not aware of the School's position or where his or her personal view may differ from that of the School, the message should state that the opinion expressed is that of the writer and does not necessarily reflect the views of the School.
• The following are prohibited:
    - "Spamming" or sending unsolicited commercial electronic messaging in accordance with the SPAM Act 2003
    (Sending junk, unwanted mail via email)
    - "Spoofing" or deliberately changing the "sender" field of email
• If a user receives a suspicious email, then the user should immediately delete the email from the Inbox and the Deleted Items box. If unsure always contact the ICT technician before opening the document.
• Email attachments should be limited in size. Large files (containing multimedia content) should not be sent via email.
• Use of Gmail, Yahoo and Hotmail (or any other third party email service) onschool equipment must follow the same protocols as school email accounts.
• Students and Staff are reminded that they have signed a **Communications Technology Agreement.** They contain a list of terms and conditions including that the computer/notebook will not be used for illegal purposes.

THE INTERNET

INTERNET ACCESS

• Users can only gain Internet access once they have logged into the Network.
• The Network Administrator may from time to time access the volumes of Internet activity by users and the sites used by users. Users should be aware that Internet usage is logged and any concerns passed to the Principal.

INTERNET USE

• The use of the Internet should be consistent with the vision, mission, values and policies of the School.
• Users should be aware that any software, games, music or movies downloaded from the Internet should be able to be used legally by the School. If a User is unsure of the licensing of Internet downloads, then they should refer to the Software Purchasing Policy and speak with the Network Administrator. This will ensure that the School has the legal license to the software and is complying with copyright law.
• The School has Internet blocking software. However, users should be aware that no blocking software is fully secure.

SURVEILLANCE AND SECURITY

SECURITY

• The ICT technician is constantly reviewing and updating Internet and word blocking software.
• If a student or staff member comes across an inappropriate/unacceptable site, they are asked to inform the Network Administrator who can manually block the website address.
• All computers at Bayview have antivirus software. When Bayview computers are connected to the Bayview network, they have a 24 hour antivirus checking surveillance system. This system is updated every 2 hours only when staff or students are logged on to the Network. It will automatically update their virus checking software if it is installed on the machine.
• If a User accidentally receives or gains access to a virus, then the User should immediately contact the ICT staff for advice on what to do.
• If a User receives a suspicious email, then the User should immediately delete the email from the In box and the Deleted Items box.
• BAYVIEW has secure hardware and software firewalls to stop intrusions.
• BAYVIEW has a disk based back up system for the whole network. Data is kept for a minimum of 10 days on a rotational basis.
Users are asked to notify the Network Administrator immediately if they become aware of any incident that could affect the security of the Network.

SURVEILLANCE

• The School encourages the use of electronic communications and respects the privacy of users. It does not routinely inspect, monitor or disclose email communications without the request of the Principal.
• From time to time the Network Administrator will be required to conduct an audit to ensure that the School's facilities, resources and services are all being used appropriately and comply with the law. This is often at the request of the Principal.
• The desktop or laptop computers supplied to staff remain the property of the School and we reserve the right to confiscate a Notebook and to delete any unsuitable material found on a Notebook.
• The Directory Service keeps a log recording which Users have been logged into the network and when.

SOFTWARE

• Bayview uses Microsoft Windows 7(?) on all computers and notebooks. Windows 7 allows Microsoft to check for unsolicited/pirated Microsoft programs on computers and notebooks when they are logged into the Internet. Users should be aware that fines for breaching copyright are very expensive.
• Users must only use software on Bayview machines that is licensed to the School.

INTELLECTUAL PROPERTY/COPYRIGHT

• Users should respect the intellectual property rights of others. In particular, users should be conscious of the provisions of the Australian Copyright Act.
• All texts, photographs, video clips, audio clips, music, movies, games and computer software are protected by copyright. Unauthorised copying, distribution or downloading of this type of material can constitute breach of copyright.
• Any material downloaded from the internet needs to be cited fully in any work submitted by a student.

HARDWARE

• All computer facilities, including notebook computers, desktop computers, scanners, and printers, digital cameras (both still and moving) are expensive, sensitive and must be treated carefully.
• Users are asked to forward all repairs or problems with hardware to the ICT technician promptly. Please do not attempt to repair equipment yourself as this is in breach of the insurance policy.

STUDENT ACCESS

• Both during and outside class time, students should take responsibility for their own use of the Network and their allocated computer. Teachers play a supervisory role in the class room but the ultimate responsibility rests with the student. Parents should remain vigilant regarding their son or daughters communication technology use outside of class time.

• Parents and guardians share with the School the responsibility for setting and conveying the standards that students should follow when using communication technologies.

BREACH OF THIS POLICY

• In accordance with the Student Code of Conduct, breaches of the **Communications Technology Agreement** will be dealt with case by case. Any disciplinary action will be decided upon by the Principal or the relevant delegate.

MOBILE PHONE

Bayview recognises that there are times when it is appropriate and useful for staff and students to have access to a mobile phone. **It is neither necessary, nor acceptable however, for mobile phones to be switched on or used during lesson or study times unless specifically linked to the teaching & learning process.**

It is the responsibility of students who bring mobile phones to school to adhere to the guidelines outlined in *Acceptable Use Policy for Student Use of Mobile Phones.* The decision to provide a mobile phone should be made by parents or guardians and as such parents should be aware if their son or daughter takes a mobile phone to school.

Parents are reminded that in case of emergency, the School's main contact number, 5523 1042 remains a vital and appropriate point of contact and can ensure your son or daughter is reached quickly and assisted in an appropriate way.

Should a student use a mobile phone inappropriately, the student will face consequences as sanctioned by the Principal, as outlined in the *Student Code of Conduct.*

MP3/IPOD/Wireless Connected Devices

Bayview recognises that there are times when it is appropriate and useful for students to have access to a Portable Audio-visual device such as an iPod, iTouch or other MP3 player or wirelessly connected device. It is neither necessary, nor acceptable however, for these devices to be switched on or used during lesson times without the express permission of the teacher in charge. Teaching staff may use portable devices to facilitate learning by disseminating lesson material via pod casting or other electronic means.

Should a student use a device inappropriately, the student will face consequences as sanctioned by the Principal, as outlined in the *Student Code of Conduct.*

REFERENCES/OTHER RESOURCES
VIEU Policy on Internet and email use in schools

USEFUL LINKS
Australian links
• **Netalert**: a toll free helpline and web site for parents wanting to ensure safe Internet usage by their young people. A Federal Government project.
http://www.netalert.net.au
• **Australian Families Guide to the Internet**: from the Australian Broadcasting Authorityhttp://www.aba.gov.au/family/index.html
• **The Child Safety Network of Australia**
http://www.childsafe.net.au/
• **Copyright Australia** has a website that details all copyright information for Australia and overseas.
www.copyright.org.au
• **SPAM ACT 2003** relevant websites for this are available at www.aca.gov.au and www.noie.gov.au

International links

• **The Responsible Netizen**
Effective strategies to assist young people in acquiring knowledge, decision making skills, motivation, and self control to behave in a safe, responsible and legal manner when using the Internet and other information technologies.
http://netizen.uoregon.edu/
• **Net Safe New Zealand: Protecting our kids on the Internet**
http://www.netsafe.org.nz/ http://www.netsafe.org.nz/
• **ChildNet International**
http://www.childnet-int.org/
• **Netaware: Safe Use of the Internet**
http://www.netaware.org/
• **SafeTeens**: Teen Safety on the Internet
http://www.safeteens.com/safeteens.htm
• **Net Parents**:
http://www.netparents.org/

ASSOCIATED DOCUMENTATION
Student Code of Conduct
Communications Technology Agreement
Harassment Policy
Software Purchasing Policy
Insurance documentation