GUIDELINES

eSMART USE OF ICT GUIDELINES

Definitions of terms used in these guidelines.

a. '**Authorised user'** means a person who has signed BYOD Permission Letter (or has had it signed on their behalf by a parent) and is authorised by the school to use school ICT.
b. **'eSmart'** refers to the name of the cybersafety guidelines that are followed at Echuca College to promote the safe, responsible and ethical use of ICT.
c. **'ICT'** stands for 'Information and Communication Technologies' and includes network facilities, communication technologies, eLearning tools and ICT equipment/devices.
d. **'Network facilities'** includes, but is not limited to, internet access to files, web sites and digital resources via the school network.
e. **'Communication technologies'** includes, but is not limited to, communication made using ICT equipment/devices such as internet, email, instant messaging, online discussions/surveys and mobile phone activities and related applications.
f. **'eLearning'** refers to the use of ICT for educational purposes.
g. '**ICT equipment/devices'** include, but are not limited to, computers (such as desktops, laptops, tablets), storage devices (such as USB and flash memory devices, CDs, DVDs, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, and any other, similar, technologies as they come into use.
h. **'Agreement'** refers to the eSmart Agreement which will be reviewed annually.
i. '**School'** means Echuca College.
j. **'School related activity'** includes, but is not limited to, an excursion, camp, sporting or cultural event, wherever its location.
k. **'School ICT'** refers to any ICT owned or operated by the school including, but not limited to, network infrastructure, computers, cameras, tablet devices.
l. **'Objectionable material'** includes, but is not limited to, pornography, cruelty, violence, or material of a discriminatory nature that it is likely to be detrimental to the wellbeing of students or unsuitable to a school environment.
m. **'Unacceptable student conduct'** includes, but is not limited to, malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, non-sanctioned gaming, impersonation/identity theft or copyright infringement.
n. **'Educational purposes'** means activities that are directly linked to curriculum related learning.
o. **'Personal electronic devices'** includes, but is not limited to, handheld gaming consoles (including but not limited to Nintendo DS, PSP Wii U), MP3 players (including but not limited to iPad, iPod, iPod Touch), e-readers (including but not limited to Kindle, Kobo) other internet and 3G accessible devices, and any other similar such devices as they come into use.
p. **'BYOD'** stands for Bring Your Own Device

Purpose

Our aim is to provide an educative environment by establishing an eSmart culture which is in keeping with the values of the school, legislative and professional obligations, and the community's expectation. Within this context, the objectives of these guidelines are to ensure the smart, safe, responsible use of ICT within the school community.

These guidelines outline the conditions applying to the use of all school ICT and behaviours associated with safe, responsible and ethical use of technology. Authorised users are required to comply with the Agreement.

Echuca College
DIVERSITY AND STRENGTH

GUIDELINES

USER eSMART OBLIGATIONS

1. Authorised Usage and eSmart Agreement

1.1. As the school provides network access, the contents of the school ICT system, including email messages, remain the property of the DET. The school has the capacity to monitor and control the system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.

1.2. All users, whether or not they make use of network facilities and communication technologies on school owned or personal ICT equipment/devices, will be issued with this Agreement. This document should be read carefully with the acknowledgement page signed and returned to the student's class teacher.

1.3. The school's ICT, including network facilities, communication technologies, and ICT equipment/devices cannot be used until the acknowledgement page of this Agreement has been signed and returned to the student's class teacher. Signed Agreements will be filed in a secure place.

1.5. The school encourages anyone with a query about these guidelines or the Agreement to contact your child's class teacher in the first instance.

2. Obligations and requirements regarding appropriate use of ICT in the school learning environment

2.1. While at school, using school owned or personal ICT equipment/devices is for educational purposes only.

2.2. When using school or privately owned ICT on the school site or at any school related activity prohibited use includes, but is not limited to, any conduct that is defined as objectionable and inappropriate:

- Would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, sexism,
- Is derogatory or threatening to another e.g. libelous, slanderous, inflammatory, threatening, harassing;
- Has intention to deceive, impersonate or misrepresent;
- Forwards confidential messages to persons to whom transmission was never authorised by the school, including persons within the school community and persons/organisations outside the school community
- Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus
- Breaches copyright
- Attempts to breach security and infrastructure that is in place to protect user safety and privacy
- Results in unauthorised external administration access to the school's electronic communication
- Propagates chain emails or uses groups or lists inappropriately to disseminate information
- Inhibits the user's ability to perform their duties productively and without unnecessary interruption,
- Interferes with the ability of others to conduct the business of the school
- Involves malicious activity resulting in deliberate damage to school ICT and/or ICT equipment/devices.
- Involves the unauthorised installation and/or downloading of non-school endorsed software
- Breaches the ethos and values of the school
- Is illegal

2.3. In the event of accidental access of such material, Authorised Users must:

- Not show others
- Shut down, close or minimise the window
- Report the incident immediately to the supervising teacher.

2.4. A person who encourages, participates or otherwise knowingly acquiesces in prohibited use of school, or privately owned communication technologies, on the school site or at any school related activity, may also be found to have engaged in prohibited use.

2.5. While at the school or a school related activity, Authorised Users must not have involvement with any material which might place them at risk. This includes images or material stored on privately owned ICT equipment/devices brought onto the school site, or to any school related activity such as USB sticks.

2.6. Authorised Users must not attempt to download, install or connect any unauthorised software or hardware onto school ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies that are available. Any Authorised Users with a query or a concern about that issue must speak with the relevant class teacher or subject teacher.

3. Monitoring by the School

The school:

3.1. Reserves the right at any time to check work or data on the school's computer network, email, internet, computers and other school ICT equipment/devices, without obtaining prior consent from the Relevant Authorised User.

3.2. Reserves the right at any time to check work or data on privately owned ICT equipment on the school site or at any school related activity. The Authorised User agrees to promptly make the ICT equipment/device available to the school for purposes of any such check and to otherwise co-operate with the school in the process. Before commencing the check, the school will inform the Authorised User of the purpose of the check.

3.3. Has an electronic access monitoring system, through Netspace (in accordance with DET requirements), which has the capability to restrict access to certain sites and data.

3.4. Monitors traffic and material sent and received using the school's ICT infrastructures. From time to time this may be analysed and monitored to help maintain an eSmart learning environment.

3.5. From time to time conduct an internal audit of its computer network, internet access facilities, computers and other school ICT equipment/devices, or may commission an independent audit of content and usage.

4. Copyright, Licensing, and Publication

4.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Authorised Users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos, images.

4.2. All material submitted for internal publication must be appropriate to the school environment and copyright laws.

4.3. Any student/s found to use an ICT equipment/device to gain advantage in exams or assessments will face disciplinary actions as sanctioned by the school.

5. Individual password logons to user accounts

5.1. If access is required to the school computer network, computers and internet access using school facilities, it is necessary to obtain a user account from the school.

5.2. Authorised Users must keep usernames and passwords confidential and not share them with anyone else. A breach of this rule could lead to users being denied access to the system.

5.3. Authorised Users must not allow another person access to any equipment/device logged in under their own user account. Material accessed on a user account is the responsibility of that user. Any inappropriate or illegal use of the computer facilities and other school ICT equipment/devices can be traced by means of this login information.

5.4. Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Guidelines and Agreement. This includes ensuring that no electronic communications could cause offence to others or harass or harm them, put the owner of the user account at potential risk, contain objectionable material or in any other way be inappropriate in the school environment.

5.5. For personal safety and having regard to Privacy laws, Authorised Users must not reveal personal information about themselves or others online. Personal information may include, but is not limited to, home addresses and telephone numbers.

6. Other Authorised User obligations

6.1. Avoid deliberate wastage of ICT related resources including bandwidth, through actions such as unnecessary printing and unnecessary internet access, uploads or downloads.

6.2. Avoid involvement in any incident in which ICT is used to send or display electronic communication, graphics, audio, video files which might cause offence to others and/or involve objectionable material.

6.3. Abide by copyright laws and obtain permission from any individual before photographing, videoing or recording them.

7. Privacy

7.1. School ICT and electronic communication should never be used to disclose personal information of another except in accordance with the school's privacy agreement or with proper authorisation. The Privacy Act requires the school to take reasonable steps to protect the personal information that is held by the school from misuse and unauthorised access. Authorised Users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.

7.2. While after school use of communication technologies by students is the responsibility of parents, school policy requires that no student attending the school may identify, discuss, photograph or otherwise publish personal information or personal opinions about school staff, fellow students or the school. Any such behaviour that impacts negatively on the public standing of the school may result in disciplinary action.

The school takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, YouTube, Tumblr (and any further new technology).

8. Procedures for Mobile Phone and Other Electronic Device Use at School

Echuca College accepts that some parents provide their children with mobile phones and other personal electronic devices. However, whilst on school property and during school excursions and camps, use of mobile phones or personal electronic devices is not permitted by students unless specifically authorised by the Principal.

Responsibility

8.1. It is the preference of the school that mobile phones are not to be brought to school

8.2. It is the responsibility of students who do bring mobile phones or personal electronic devices onto school premises to adhere to the guidelines outlined in this document.

8.3. The decision to provide a mobile phone or personal electronic device to their children should be made by parents or guardians.

8.4. The school accepts no responsibility for replacing lost, stolen or damaged mobile phones or personal electronic devices. Their safety and security is wholly in the hands of the student.

8.5. The school accepts no responsibility for students who lose or have their mobile phones or personal electronic devices stolen while travelling to and from school.

8.6. It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.

8.7. Students must protect the privacy and dignity of individuals and security of information, to maintain the public standing of the school and compliance with State and Federal laws.

8.8. The school strongly advises that for safety reasons headphones should not be used when students are traveling to and from school, eg. walking, riding a bike, moving on and off buses.

Parents are reminded that in cases of emergency, the school office remains a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in the appropriate way.

Breach of Guidelines

Breaches of these Guidelines will be dealt with in accordance with the school Student Engagement and Wellbeing Policy.

This policy was last ratified by School Council on....	4th June 2015