WCB eLearning and eSmart Policy

Definition:

- This Policy and Agreement outlines the conditions applying to the use of all college ICT and behaviours associated with safe, responsible and ethical use of technology. Authorised users are required to comply with the Agreement.

Rationale:

- Cybersafety is an important issue for all students. In addition, students may be bringing personal devices to school for educational purposes. By the time students arrive at secondary school most will already be regular and active users of digital technologies including social media tools. Safe use of devices and digital learning environments is important.

Aims:

- The college's aim is to provide an educative environment by establishing an eSmart culture which is in keeping with the values of the college, legislative and professional obligations, and the community's expectation. Within this context, the objective of this Policy and Agreement is to ensure the smart, safe, responsible use of ICT within the college community.

Implementation:

1.1 All staff At Weeroona College Bendigo:

- Support the rights of all members of the school community to engage in and promote a safe, inclusive and supportive learning environment.

- Support the Student Engagement & Wellbeing Policy that clearly states our school's values and the expected standards of student behaviour, including actions and consequences for inappropriate behaviour.

- Educate our students to be safe and responsible users of digital technologies.

- Raise our students' awareness of issues such as online privacy, intellectual property and copyright.

- Supervise students when using digital technologies for educational purposes.

- Provide a filtered internet service but acknowledge that full protection from inappropriate content can never be guaranteed.

- Respond to issues or incidents that have the potential to impact on the wellbeing of our students.

- Know that some online activities are illegal and as such we are required to report this to the police.

- Provide parents/guardians with a copy of the college's *Acceptable Use Agreement* as needed.

- Support parents/guardians to understand the importance of safe and responsible use of digital technologies, the potential issues that surround their use and strategies that they can implement at home to support their child.

1.2 Breach of Acceptable Use Agreement

Breaches of the Acceptable Use Agreement can undermine the values of the college and the safety of the eLearning environment, especially when ICT is used to facilitate misconduct. Such a breach which is deemed by the college to be harmful to the safety of the college may possibly result in serious disciplinary action such as

1. Withdrawal of access to the college network and devices for a period of time.
2. Confiscation of personal devices used inappropriately throughout the school day, including on college buses, at sport, and during camps/excursions.
3. Suspension or withdrawal of enrolment in cases of serious misconduct
4. It is a criminal offence to use an ICT device to menace, harass, make threats, or offend another person. In these instances, the college may consider it appropriate to involve police.

In investigating a suspected breach of this Policy and Acceptable Use Agreement, the Authorised User agrees to promptly make the ICT equipment/device available to the college for the purpose of any investigation and/or audit and to cooperate otherwise with the college in any investigation or audit process.

The terms of this Policy and Acceptable Use Agreement form part of the college's expectations for the purposes of a student's enrolment at the college and the conditions of enrolment.

1.3 User eSmart Obligations

Authorised Usage and eSmart Agreement

- As the college provides network access, the contents of the college ICT system, including the college Intranet and email messages, remain the property of the college. The college 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.

- All users, whether or not they make use of network facilities and communication technologies on college owned or personal ICT equipment/devices, will be issued with this Acceptable Use Agreement. The document should be read carefully with the Student Commitment page signed and returned to your student's Learning Advisor.

- The college's ICT, including network facilities, communication technologies, eLearning tools and ICT equipment/devices cannot be used until the Student Commitment page of this Acceptable Use Agreement has been signed and returned to your student's Learning Advisor. Signed Agreements will be filed in a secure place.

- It is recommended that authorised users keep the eSmart Policy and Acceptable Use Agreement for reference. If necessary, a replacement copy will be supplied upon request.

- The college encourages anyone with a query about the eSmart Policy and/or Acceptable Use Agreement to contact your child's Learning Advisor.

1.4 Obligations and requirements regarding appropriate use of ICT in the college learning environment

1.4.1. While on campus, using college owned or personal ICT equipment/devices is for educational purposes only.

1.4..2. When using college or privately owned ICT on the college site or at any college 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. libellous, slanderous, inflammatory, threatening, harassing
- Has intention to deceive, impersonate or misrepresent
- Forwards confidential messages to persons to whom transmission was never authorised by the college, including persons within the college community and persons/organisations outside the college 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 college'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 college
- Involves malicious activity resulting in deliberate damage to college ICT and/or ICT equipment/devices.
- Involves the unauthorised installation and/or downloading of non-college endorsed software
- Breaches the ethos and values of the college

1.4.3. 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 classroom teacher.

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

1.4.5. While at the college or a college 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 college site, or to any college related activity such as USB sticks.

1.4.6. Authorised users must not attempt to download, install or connect any unauthorised software or hardware onto college 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.

1.4.7. Use of personal devices during the school day is at the discretion of teachers and staff. Students must use these devices as directed by their teacher.

1.4.8. The primary purpose of the use of personal devices at school is educational.

1.4.9. The use of a personal device is not to be a distraction in any way to teachers or students. The use of personal devices must not disrupt class in any way.

1.4.10. Students must bring their device to school fully charged and are not permitted to charge their device at school.

1.4.11. Students agree not to attempt to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.

1.4.12. Students shall not distribute pictures or video of students or staff without their express permission.

1.5 Monitoring by the College
The college:
- Reserves the right at any time to check work or data on the college's computer network, email, internet, college Intranet, computers and other college ICT equipment/devices, without obtaining prior consent from the Relevant Authorised User.

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

- Has an electronic access monitoring system, IAM (Internet access Monitor), which has the capability to restrict access to certain sites and data, record email and internet use, including the user details, time, date, sites visited, length of time viewed, and from which computer or device.

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

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

1.6 Copyright, Licensing, and Publication

1.6.1. 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 and images.

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

1.6.3. 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 college.

1.7 Individual password logons to user accounts

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

1.7.2. 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.

1.7.3. 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 college ICT equipment/devices can be traced by means of this login information.

1.7.4. Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Policy 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 college environment.

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

1.8 Privacy

1.8.1. College ICT and electronic communication should never be used to disclose personal information of another except in accordance with the college's privacy protocols or with proper authorisation. The Privacy Act requires the college to take reasonable steps to protect the personal information that is held by the college 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.

1.8.2. While **after school use** of communication technologies by students is the responsibility of parents, college policy requires that no student attending the college may identify, discuss, photograph or otherwise publish personal information or personal opinions about college staff, fellow students or the college. Any such behaviour that impacts negatively on the high public standing of the college may result in disciplinary action. The college takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, You Tube, Tumblr (and any further new technology).

1.9. Procedures for Mobile Phone Use at School

Weeroona College Bendigo accepts that parents provide their children with mobile phones to protect them from everyday risks involving personal security and safety. There is also ever-increasing concern about children travelling alone on public transport or commuting long distances to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can speak with their child quickly, at any time.

However, while on campus, using college owned or personal ICT equipment/devices, including mobile phones, is for educational purposes in the first instance to ensure the benefits that mobile phones provide (such as increased safety and security) can continue to be enjoyed by our students.

For further information, please refer to 'Weeroona College Bendigo Mobile Phones and Similar Electronic Devices Policy.'

Parents are reminded that in cases of emergency, the college's General Office remains a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in the appropriate way. Phone calls home to parents are to be made through the General Office.

1.10. **Student Owned Devices**

1.10.1 Personal devices can enhance and enrich learning opportunities both at home and at school. Weeroona College Bendigo is committed to allowing responsible, learning centred use of personal devices at school so as to provide as many pathways to understanding as possible for our students.

1.10.2 **Access to the** Weeroona College Bendigo **wireless guest network is a privilege, not a right**. Any use of the wireless network entails personal responsibility and compliance with all school rules and the Weeroona College Bendigo Acceptable Use Policies. In using the Weeroona College Bendigo network you willingly grant IT staff permission to conduct any necessary investigations regarding inappropriate Internet use at any time.

1.10.3 **School Liability Statement**
- **Students bring their own personal devices to use at Weeroona College Bendigo at their own risk**. It is their duty to be responsible in the upkeep and protection (anti-virus software / security settings) of their devices.
- A locker will be provided for the storage of student equipment and devices when not in use. Students are responsible for providing and using locks on their locker.
- **Weeroona College Bendigo will NOT be responsible for:**
  - Personal devices that are broken/damaged while at school or during school-related activities. Should a student's device be damaged in a situation out of their control at school the College will investigate offer support as appropriate.

- o Personal devices that are lost or stolen at school or during school-related activities. Should a student's device be stolen at school the College will investigate offer support as appropriate.
- o Maintenance or upkeep of any personal device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues). School licensed software will not be installed on student personal devices.
- o Any possible device charges to your account that might be incurred during approved school-related use.

1.10.4 The college will offer the following support for students.
- We will offer technical advice as required.
- The College will monitor internet access of all students.
- We will educate students on protecting their device.
- We aim to access free apps. Paid apps will be restricted and have an approval process through our Student Learning Team.

1.10.5. Student Responsibilities
- Students will be expected to take all practical steps to protect their device.
- The College expects that all students will use age appropriate apps and sites to support their learning at the College.

How else can parents assist?
- Reinforce the eSmart policy with your child
- Encourage your child to comply with the college's eSmart policy
- Call or message your child only during lunch breaks, if necessary.
- Support the college in the enforcement of the eSmart policy

Definitions of terms used in this Policy and Agreement.

a. '**Authorised user**' means a person who has signed the eSmart Agreement (or has had it signed on their behalf by a parent) and is authorised by the college to use college ICT.

b. **'eSmart'** refers to 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, intranet and internet access to files, web sites and digital resources via the college wireless network.

e. **'Communication technologies'** includes, but is not limited to, communication made using ICT equipment/devices such as internet, intranet, email, instant messaging, online discussions/surveys and mobile phone activities and related applications.

f. **'eLearning tools'** includes, but is not limited to, Edustar software and any online applications and programs that are used 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. **'college Intranet'** is the college's network drive.

i. '**Acceptable Use Agreement'** refers to the Acceptable Use Agreement Weeroona College Bendigo.

j. **'College'** means Weeroona College Bendigo.

k. **'College related activity'** includes, but is not limited to, an excursion, camp, sporting or cultural event, wherever its location.

l. **'College ICT'** means the college's ICT including network facilities, communication technologies, eLearning tools and ICT equipment/devices.

m. **'Objectionable material'** deals with matters such as pornography, cruelty, violence, or material of a discriminatory nature that it is likely to be injurious to the good of students or incompatible with a college environment.

n. **'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, copyright infringement, or cheating in an examination.

o. **'Educational purposes'** means activities that are directly linked to curriculum related learning.

Related documents/policies-
- Acceptable Use Agreement Weeroona College Bendigo 2013
- Weeroona College Bendigo Mobile Phones & Similar Electronic Devices Policy 2011
- School Community Wellbeing Policy 2011 (Anti Bullying & Harassment Policy)

This policy was last ratified by School Council	**April 2013**	