Policy:	*eSmart Policy*
School:	*Benalla P-12 College*
Section:	*Curriculum 4.5*
Version:	*One*

Basic Beliefs:

This eSmart Policy is built on the necessity for educating and protecting all members of the Benalla P-12 College community. The college values of Respect, Responsibility, Integrity and High Expectations are essential components of this cyber wellness document, which includes the rights and responsibilities of all members of the college community.

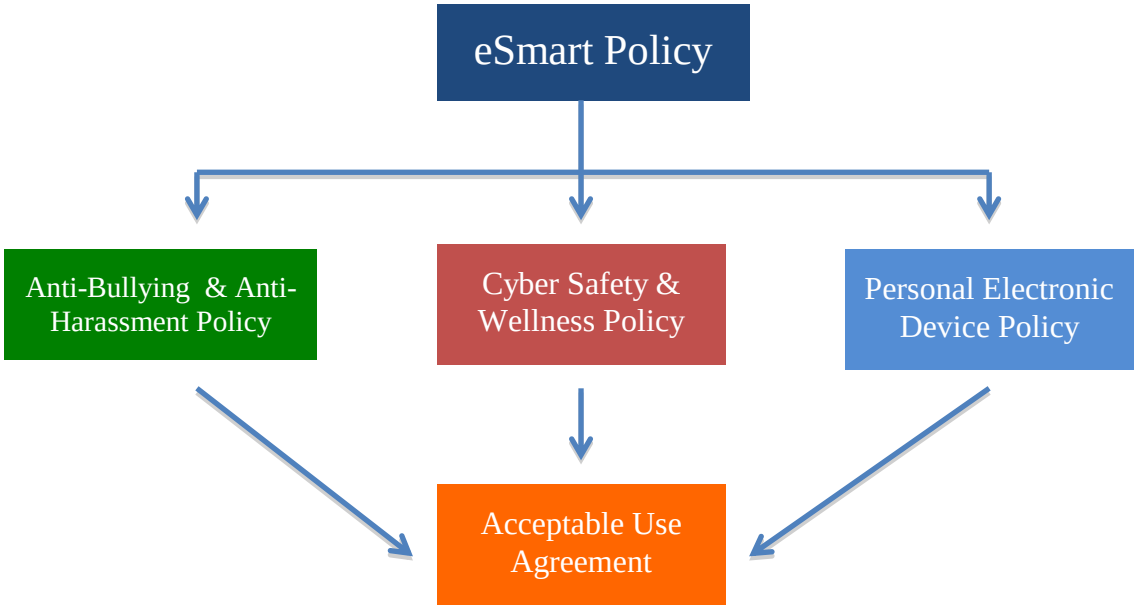
The college's computer network, internet access facilities, computers and other college ICT equipment/devices, such as student netbooks or iPads, bring great benefits to the teaching and learning programs at Benalla P-12 College, and to the effective operation of the college. However, it is essential that the college endeavours to ensure the safe use of ICT within the college community.

Implementation:

To establish clear policies and guidelines around the use of technology and cyber wellness for all members of the Benalla P-12 College community.

Documentation in this policy:

1. Anti-Bullying & Anti-Harassment Policy
2. Cyber Safety & Wellness Policy
3. Personal Devices Policy
4. Acceptable Use Agreement



This eSmart policy includes information about obligations, responsibilities, and the nature of possible consequences associated with breaches of the 'Use Agreement', which undermines the safety of the college environment. The cyber wellness education supplied by Benalla P-12 College to its learning community is designed to complement and support the use of this policy. The overall goal of the college is to create and maintain a culture of cyber wellness. All members of the college community benefit from being party to the 'Use Agreement' and other aspects of the college eSmart policy.

1. Anti Bullying and Anti Harassment Policy

Agreed Understandings:

The school has the responsibility to foster an education environment where every attempt is made to eliminate barriers to learning and where all feel safe and valued. Our school has a 'zero tolerance' to bullying and harassment and is committed to working towards the eradication of these behaviours from the school community.

Definition:

A person is bullied when they are exposed regularly and over time to negative actions on the part of one or more persons. Bullying behaviour is that which deliberately sets out to intimidate, exclude, threaten and/or hurt others, typically on a repeated basis. Bullies can operate alone or as a group. Bystander bullying is being part of a group where bullying behaviours are occurring and the bystander/s do not take preventative or discouraging action. Cyberbullying is when someone is tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted by another individual using the internet, interactive and digital technologies or mobile phones.

Types of Bullying

There are four broad categories of bullying:-

1. **Direct physical bullying** e.g. hitting, tripping, and pushing or damaging (or causing to be damaged) an individual's property. This also includes intimidating body language.

2. **Direct verbal bullying** e.g. name calling, insults, homophobic or racist remarks, verbal abuse.

3. **Covert bullying** - This is harder to recognise and often carried out behind the bullied person's back. It is designed to harm someone's social reputation and/or cause humiliation. Indirect bullying includes:
    - lying and spreading rumours
    - playing nasty jokes to embarrass and humiliate
    - mimicking
    - encouraging others to socially exclude someone
    - damaging someone's social reputation and social acceptance
4. **Cyber Bullying** - Involves the use of email, text messages, pictures, video recordings or chat rooms to humiliate intimidate and/or distress.

Guidelines:

1. Bullying may occur between various members of a school community (students, staff, parents and volunteers). Policy implementation strategies must be developed and owned by the entire college community and apply during excursions, camps and all on and off site activities.

2. This policy also relates to the school's policies on use of mobile phones and other electronic devices, the OHS policy, Student Well-being and Engagement Policy and all Department policies related to the wellbeing of staff, students and school community.

Implementation:

1. All staff will undergo professional development which addresses prevention and management of bullying behaviour and staff responsibilities, concerning this issue.

2. Individuals will be encouraged to report incidences of bullying to a staff member. Staff and students will be trained in how to recognise the signs or evidence of bullying. Staff and students will be informed that it is their responsibility to report bullying whether the person is an observer or victim.

3. General management will include the regular discourse between staff, students and parents.

4. Bullying incidences should be immediately discussed, reported and accurately recorded on a "Behavioural Report" form. This will be completed using the School Management System, Sentral – Incident Reporting.

5. Specific bullying incidents may be managed by no blame, restorative or punitive approaches following the procedures contained within the Student Engagement and Well-being Policy.

6. Preventative strategies such as playground changes and appropriate classroom strategies will be monitored and adjusted accordingly.

7. Preventative programs and structures such as an anti-bullying curriculum and parent education e.g. Cyber Safe will be implemented.

8. The education of our school community will involve consistent references to our school values, in order to support the development of a wider, caring school community. Newsletters will contain updates about what constitutes bullying, how to help victims and bullies, communication with the school, how the school responds to bullying, parent sessions and counselling.

9. The policy will be made available on the school website

Resources

- *Safe Schools are Effective Schools* (http://www.eduweb.vic.gov.au/edulibrary/public/stuman/wellbeing/SafeSchoolsStrategy.pdf)
- *Bullying Solutions :Evidence based approaches to bullying in Australian schools* – McGrath H & Noble T (ed)
- *Don't be a Bully Bystander* – Ryebuck Media

2. Cyber Safety & Wellness Policy

Agreed Understandings:

It is important for young people to understand the morals and ethics of using technology to access online content, and we therefore acknowledge that we have a moral obligation to teach students about responsibility and accountability in the use of **technology in the classroom** and beyond. We believe that all members of our school community have an important role to play in teaching and monitoring their child's use of technology. We will focus on developing positive well-being for Internet users and an awareness of how to protect oneself and others from harmful online behaviour.

Guidelines:

1. Use of Social Media

1.1 Students must not use social media to threaten, bully, intimidate or otherwise harass other people through any SMS or text message, photographic, video or other data transfer system available on the phone or for any illegal activity. Such inappropriate activities will incur disciplinary action including suspension and the police contacted.

1.2 All material submitted on social media sites should be appropriate to the college environment.

2. Requirements regarding appropriate use of ICT in the College learning environment

In order to meet the college's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the college:

2.1. The use of **the college's** computer network, Internet access facilities, computers and other college ICT equipment/devices, including but not limited to iPads and student netbooks or notebooks, on *or* off the college site, is limited to educational purposes appropriate to the college environment. This applies whether or not the ICT equipment is owned/leased either partially or wholly by the college.

2.2. The college has the right to, and will monitor, access, and review all the use detailed in 2.1. The college will use remote access software to ensure appropriate use of ICT devices and the college network. This includes personal emails sent, received and images stored on the college's computers and/or network facilities, either during or outside college hours.

2.3. The use of any **privately-owned/leased** ICT equipment/devices on the college site, or at any college-related activity must be appropriate to the college environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the college site, or to any college-related activity.

Such equipment/devices could include a netbook, notebook, desktop, iPads, mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone

unsure about whether or not it is appropriate to have a particular device at school or at a college-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the ICT Management Team.

PLEASE NOTE: Examples of a 'college-related activity' include, but are not limited to, an excursion, camp, sporting or cultural event, wherever its location.

2.4. **When using a global information system** such as the Internet, it may not always be possible for the college to filter or screen all material. This may include material which is **inappropriate** in the college environment (such as 'legal' pornography), **dangerous** (such as sites for the sale of weapons), or **illegal material***.*

3 Monitoring by the college

3.1. Benalla P-12 College has an electronic access monitoring system which has the capability to record Internet use, including the user details, time, date, sites visited, and from which computer or device the http traffic was viewed. The ICT Management Team also has the ability to remotely monitor college ICT equipment, via logs and real-time screen viewing, including student netbooks, notebooks and iPads. You must not attempt to prevent the ICT Management Team from remotely monitoring any ICT equipment/device.

3.2. The college has tracking, geo location, theft prevention and recovery software installed on all ICT equipment. This software will record the location of all ICT devices and will be activated to recover stolen or lost equipment.

3.3. The college will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.

3.4. The college holds the right to access/redirect/stop/copy for evidence, any type of electronic data and remove inappropriate electronic data without notice.

3.5. The college holds the right to lock/disable/remove/modify domain/local computer accounts in the event of a threat to the college ICT security. This includes any electronic devices which are on the premises of the college.

4. Ownership

4.1 Netbooks remain the property of the college. Students may not purchase netbooks for use on the college system.

4.2 Personal Devices will remain the responsibility of the owner. Benalla P-12 College will not be liable for any financial costs associated with personal devices.

4.3 If any privately-owned ICT equipment/device, such as; netbooks, iPads, mobile phone, camera, or recording device, portable storage (like a USB or flash memory device), is brought to college or a college-related activity, the college cyber wellness rules apply to that device.

5. Breaches of the Use Agreement

5.1. Breaches of the 'Use Agreement' can undermine the values of the college and the safety of the learning environment, especially if ICT is used to facilitate misconduct.

5.2. Such a breach which is deemed harmful to the safety of the college, such as involvement with inappropriate or illegal material, anti-social activities such as harassment and bullying and possession of peer-to-peer software will constitute a significant breach of discipline and result in serious consequences. A breach of this agreement will result in the netbook, iPad or ICT device being reimaged. Any further breaches of this nature will result in changes to the management of the netbook, or ICT device. The ICT Manager and/or year level coordinator will respond and take appropriate action regarding consequences of all breaches.

5.3. Involvement with **material or behaviour** which is deemed 'age-restricted' or 'objectionable' (illegal) is a very serious matter, as is involvement in an **activity** which might constitute criminal misconduct, such as harassment. In such situations, it may be necessary to involve police in addition to any disciplinary response made by the college as a result of its investigation.

5.4 Depending on the seriousness of a particular breach of the use agreement, an appropriate

response will be made by the college. Possible responses could include one or more of the following: a discussion with the student, informing parents/legal guardian/caregiver, reimaging of the device, loss of administrator access to devices, loss of student access to college ICT, and/or the taking of disciplinary action. If illegal material or activities are involved, it may be necessary for the college to inform the police and/or other government departments.

Implementation:

Student Safe and Responsible Behaviours:

When I use digital technologies I:

- ***Communicate respectfully*** by thinking and checking that what I write or post is polite and respectful, as in line with our school values.

This means:

- ✓ Never sending mean or bullying messages or passing them on, as this make me part of the bullying.
- ✓ Not using actions online to be mean to others.
- ✓ Not copying someone else's work or ideas from the internet and presenting them as my own.

- ***Protect personal information*** by being aware that my full name, photo, birthday, address and phone number is personal information and should NOT be shared online.

This means:

- ✓ Protecting my friend's information in the same way.
- ✓ Protecting my password and not sharing it with others.
- ✓ Only joining a space online with my parent or teacher's guidance and permission.
- ✓ Never answering questions online that ask for my personal information.

- ***Look after myself and others*** by thinking about what I share online.

This means:

- ✓ Never sharing my friend's full names, birthdays, school names, addresses and phone numbers because this is their personal information.
- ✓ Speaking to a trusted adult if I see something that makes me feel upset or if I need help.
- ✓ Speaking to a trusted adult if someone is not treating me with respect.
- ✓ Stopping to think about what I post or share online.
- ✓ Being careful with the equipment that I use.

1. Personal Electronic Devices Policy

Agreed Understandings:

The use of personal electronic devices, such as; mobile phones, iPads, MP3 players and other electronic devices can be disruptive to the learning and social environment of students – if used inappropriately. Contemporary learning is enhanced when the use of these devices is present as it allows students to collaborate with staff and peers, access educational resources and develop creativity. Protocols for socially acceptable use of such devices *within a school setting* are appropriate as part of the learning process.

Guidelines for use of Personal Electronic Devices:

1. Personal electronic devices; mobile phones, iPads, mp3 players and other electronic devices must not be used in classes unless their use is directly related to the curriculum as determined by the classroom teacher. This also relates to the use of headphones in class, where these are only to be used as per the direction from the teacher.

2. Students who bring personal electronic devices to school do so at their own risk. Neither the school nor the Department of Education & Early Childhood Development has personal property insurance to cover the loss or damage to such items, and cannot provide reimbursement in this instance.

3. Personal electronic devices should not be used in any manner or place which impedes learning or causes disruption to the normal routine of the school. There is to be NO recording in any class without the teacher's permission.

4. It is important that students display courtesy, consideration and respect for others when using personal electronic devices.

5. Personal electronic devices capable of taking or recording images are not to be used anywhere a normal camera would be considered inappropriate, such as change rooms or toilets. To do so would incur sanctions under the College's eSmart Policy and may become a police matter.

6. The use of personal electronic devices used to send harassing or threatening messages is inappropriate and will be dealt with under the College's eSmart Policy and may become a police matter.

7. Appropriate sanctions apply to any student using an electronic device to cheat or gain unfair advantage in exams or assessments.

8. When a student is sent to the Sub School, they will be required to give over to the member of staff, ALL their personal devices. This includes; iPads, Phones, MP3 players, iPods.

9. Students and staff should ensure that their personal electronic devices are always stored in a safe and secure place.

10. This policy applies during excursions, camps and extra-curricular activities.

Implementation:

1. All staff, students and families will be notified of this policy via regular written and verbal communication.

2. Appropriate sanctions will apply for breaches of this policy. This will include temporary confiscation of mobile phones or other electronic devices.

Basis for discretion:

1. The basis for discretion lies with the Principal as an operational matter.

2. There may be times where exceptional circumstances occur, allowing the use of such devices, with restricted use and with the approval of the Principal. eg. When guest speakers are present and video/voice recordings are permitted on a personal device for use in later lessons.

The basis for discretion lies with the Principal as an operational matter.

Date Implemented	December, 2014

Date of ratification by School Council: **23 February, 2015**

Recommended date for review: **February, 2017**

BENALLA P-12 COLLEGE

Student ICT use Agreement

Introduction

The school's ICT equipment and devices bring great benefits to the teaching and learning at Benalla P-12 College. The College wants to create and maintain a cyber safety and wellness culture which upholds the values of the school.

STUDENT NAME: _____

YEAR LEVEL: _____

This agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber safety and wellness breaches which undermine the safety of the school environment.
The school's computer network, Internet access facilities, computers and other school ICT equipment/devices are for educational purposes appropriate to the school environment. Students and parents are asked to carefully read, and then sign the following agreement. They are also encouraged to familiarise themselves with all elements of the eSmart Policy.

Important terms used in this document:

- *The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies'*
- *The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops), storage devices (such as USBs, CDs, DVDs), cameras (such as video, digital, webcams), all types personal electronic devices (such as mobile phones, iPads, iPods, etc).*
- *The eSmart Policy refers to everything that is included in the* Anti-Bullying & Anti-Harassment Policy, Cyber Safety & Wellness Policy and Personal Devices Policy.
- The term 'parent' used throughout this document also refers to legal guardians and caregivers.

Rules to help keep Benalla P-12 College community Cyber safe.

As a safe and responsible user of ICT I will help keep myself and other people safe by following these rules

1. I cannot use school ICT equipment until my parent and I have read and signed my ICT agreement form and returned it to school.
2. I will log on only with my user name. I will not allow anyone else to use my user name.
3. I will not give anyone else my password, or use or pass on anyone else's password.
4. I will not have any involvement with any ICT material or activity which might put myself or anyone else at risk (e.g. bullying or harassing).
5. I understand that I must not at any time use ICT to upset, offend, harass, threaten or in any way harm anyone connected to the school or the school itself, even if it is meant as a joke.
6. I understand that the rules in this use agreement also apply to all personal electronic devices; mobile phones, iPads, etc.
7. I understand that I can only use the Internet at school when a teacher gives permission and there is staff supervision.
8. While at school, I will not:
    - Access, or attempt to access, inappropriate, age restricted, or offensive material.
    - Download, save or distribute such material by copying, storing, printing or showing it to other people.
    - Make any attempt to get around or bypass security, monitoring and filtering that is in place at school.
9. If I accidentally access inappropriate material, I will:
    - Not show others
    - Turn off the screen or minimise the window and
    - Report the incident to a teacher immediately.

10. I understand that I must not download any files such as music, videos, games or programmes that are copyrighted. I also understand that anyone who infringes copyright may be personally liable under copyright law.

11. I understand that these rules apply to any privately owned ICT equipment/device (personal electronic device), I bring to school or a school-related activity. Any images or material on such equipment/devices must be appropriate to the school environment.

12. I will not connect any device (such as a USB drive, camera or phone) to, or attempt to run any software on, school ICT without a teacher's permission. This includes all wireless technologies.

13. I will ask a teacher's permission before giving out any personal information (including photos) online about myself or any other person. I will also get permission from any other person involved. Personal information includes name, address, email address, phone numbers, and photos.

14. I will respect all ICT systems in use at school and treat all ICT equipment/devices with care. This includes:

    - Not intentionally disrupting the smooth running of any school ICT systems
    - Not attempting to hack or gain unauthorised access to any system
    - Following all school cyber safety and wellness rules, and not joining in if other students choose to be irresponsible with ICT
    - Reporting any breakages/damage to a staff member.

15. I understand that the school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including email.

16. I understand that the school may audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including email.

17. I understand that if I break these rules, the school may inform my parent(s). In serious cases the school may take disciplinary action against me. I also understand that my family may be charged for repair costs. If illegal material or activities are involved, it may be necessary for the school to inform the police.

18. I will follow the eSmart Policy and instructions whenever I use the school's ICT.

19. I will keep this document somewhere safe so I can refer to it in the future.

20. I will ask a teacher if I am not sure about anything to do with this agreement.

21. I understand that Benalla P-12 College and its staff will not be liable for any damages to any BYOD device whilst being used at the college.

I have read and understood my responsibilities and agree to abide by this ICT Use Agreement. I know that if I breach this use agreement there may be serious consequences.

Name of student: ..... **Home Group:** .....

Signature: ..... **Date:** .....

Section for parent/legal guardian/caregiver

I have read this ICT Use Agreement document and am aware of the school's initiatives to maintain a cyber safe learning environment, including my child's responsibilities.

Name of parent/legal guardian/caregiver: .....

Signature: ..... **Date:** ……