



eSmart Policy

Rationale

Heritage College, is committed to creating positive Digital Citizens. Being an eSmart school means using Digital Technologies in a safe and responsible manner. Students, teachers and the wider school community are equipped with the skills and knowledge to embrace and safely navigate technologies. Digital Technologies are used to enhance and develop the 21st Century Learning Skills of students, helping to prepare future ready students.

This policy should be read in conjunction with the school's Student Owned Device User Agreement and the eLearning and Technology Procedure.

Aims

- to provide a safe, secure and caring learning environment.
- to develop safe practices for the use of the internet for learning.
- to establish clear expectations for students, teachers and the community when using technology.
- to explicitly teach students safe, and responsible behaviour, and respectful online behaviours.
- to achieve accreditation as an eSmart school by meeting all criteria as outlined in the eSmart System Tools.

Definitions

Approved/School Sponsored Websites: a list of approved/appropriate digitally based communication tools/sites for staff to communicate with students and families. The sites that are approved/appropriate for communication at Heritage College are:

1. SEQTA
2. School supplied email address e.g. fristinitial.surname@heritagecollege.com.au
3. Seesaw
4. Blog/Blogger/Blogspot (any blog that is able to be locked with a password)
5. School owned FaceBook page
6. School Website
7. Class Dojo
8. 8. Google Classroom
9. Google Forms
10. Google Calendar
11. Google Drive
12. Edmodo and Edrolo
13. Twitter - with written and recorded parental consent, no names used (either first names or surnames)
14. iMaths
15. Studyladder
16. School phones - all conversations recorded in SEQTA
17. Instagram - set as private, with written and recorded parental consent, no names used (either first names or surnames)
18. Storybird Writing app (feedback app for student writing)



Bullying: "...is repeated verbal, physical, social or psychological aggressive behaviour by a person or group directed towards a less powerful person or group that is intended to cause harm, distress or fear." (As defined by the Department of Education Victoria <http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/what.aspx>)

Inappropriate/Antisocial Behaviour: is behaviour that is 'silly' - acting without thinking of others or consequences to others; 'Rude' - unintentional or hurtful and/or 'Mean' - intentional, hurtful, an isolated or single incident. (As defined in the schools Behaviour Management Policy)

Cyber: refers to the virtual online world which can be accessed through a variety of technology (computers, ipads, mobile phones, ipods).

Cybersafety: is the act of maintaining your own and others personal security and wellbeing while interacting with the online world. (It applies to your full name, address, phone number, school, age, birthday, email address).

Cyberbullying: is when an individual, or group, uses digital technology devices to intentionally hurt another person. (As defined by the Department of Education Victoria <http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/cyberbullying.aspx>)

Digital Literacies: is the knowledge, skills, and behaviours used in a broad range of digital devices such as smartphones, tablets and laptops.

Digital Citizenship: is the social skills and protocols of responsible behaviour when using technology.

Digital Footprint: is a trail left by interactions in a digital environment. In social media, a digital footprint is the size of the person's 'online presence' measured by the number of individuals with whom they interact.

Digital Literacy: is the ability to effectively and critically navigate, evaluate and create information using a range of digital technologies.

Netiquette: is the set of social conventions that facilitate interactions over networks.

Social Media: is the means of interactions among people in which they create, share and exchange information and ideas in online communities and networks (such as Facebook, Tumblr and LinkedIn).

SEQTA: is the Student Management and Curriculum Planning Tool used by Heritage College to plan learning and teaching programs and record student information.

Parent Expectations

Parents are key partners in the development of eSmart students, with the expected responsibilities of:



- Exhibiting and reinforcing safe and responsible behaviours when communicating off and online.
 - Supervising students when they are online.
 - Signing and being familiar with the school's Student Owned Device User Agreement and the eLearning and Technology Policy.
-
- Ensuring students sign and are familiar with the school's Student Owned Device User Agreement and the eLearning and Technology Procedure.
 - Supporting students to meet the expectations outlined in the school's Student Owned Device User Agreement, the eLearning and Technology Procedure and this eSmart Policy.
 - Reporting any incidents of cyberbullying or unsafe cyber-behaviour that they have become aware of happening at school to the school.
 - Meeting with staff if students are involved in cyberbullying incidents.
 - Seeking and obtaining permission before taking photos/videos of their child with another when at school or at a school related event.
 - Only share images/videos with the consent of all individuals and their parents (age appropriate).
 - When sharing images/videos (with consent), details of the individuals within the photo should not be tagged or shared.

**In the instance where 'mature minors' are capturing images/video they are to seek permission before using the image in any online platform or before sharing the image in any way.*

**When posting on any online platforms, surnames or personal details are not to be shared or tagged to the image and the image should not be altered to the detriment of any individuals within it.*

Teacher Expectations

At Heritage College, staff are expected to:

- Exhibit safe and responsible behaviours when communicating off and online as per the Adventist Schools Victoria Acceptable Use Agreement.
- Effectively supervise students while online on school digital devices.
- Provide education to students around the smart, safe and responsible use of digital technologies following the Australian Curriculum Digital Technologies Scope and Sequence reinforcing positive Digital Citizenship in their classrooms.
- Read and explain the Acceptable Use Agreement in term one each year and ensure all students accessing our network have signed it.
- Ensure that students adhere to the Acceptable Use Agreement, report and record breaches within SEQTA and follow reporting guidelines when required.
- Report all cases of cyberbullying and unsafe cyber behaviour to school leadership and record this within SEQTA.
- Report all cases of cyberbullying and unsafe cyber behaviour to parents if it is happening at home.
- Protect their passwords, guard their privacy on the internet and be aware of their digital footprint (use privacy settings and mindful of online comments).
- Ensure they are only communicating with students and families via the appropriate approved school sponsored websites. Please refer to **definitions** for a list of approved school sponsored websites for Heritage College.



- When saving images/photos of school children, staff must upload all photos to the school shared drive, school photo year book drive or onto a school owned device (e.g. staff laptop, iPad, school owned phone etc...). These images can only be stored on the staff laptop for the current year and either uploaded to the school shared drive, school photo year book drive or deleted before the end of the school year.



School Expectations

The school will provide a range of opportunities for the use of digital technologies within an educational setting. The school has a policy in place that outlines the values of the school and the expected behaviours of students, parents, staff and the school. The school provides a filtered network service and effective supervision of students while on school owned digital devices. The school provides access to age appropriate search engines and teacher recommended and reviewed websites and applications. The school uses the Australian Curriculum Digital Technologies curriculum that reflects that eSmart standards. The school provides support to students, parents and staff to understand and use digital technologies.

Incidents

Incidents of cyberbullying and unsafe online behaviour will be not tolerated at Heritage College on school grounds, school excursions, camps and extra-curricular activities. Students, parents, teachers and community members are encouraged to report an incident immediately to school leadership and/or relevant authorities where necessary if;

- they feel that the wellbeing of a student is being threatened
- they have experienced an incident of cyberbullying (see definition)
- they come across sites/texts/images/videos which are not suitable for school use
- they or someone they know accesses, makes or sends an uncomfortable text, photo, video or audio
- they or someone they know posts private information intentionally or unintentionally
- they or someone they know uses content owned by others e.g. text, images, music and video and does not acknowledge the source
- they or someone they know does not seek support when there is an issue with devices
- they or someone they know asks for private information or to meet in person
- they or someone they know deliberately damages electronic devices or settings
- they or someone they know breaks the Acceptable Use Agreement

Procedures, Reporting and Storage of Information

- Incidents are recorded by staff on SEQTA, and School Leadership are notified of any incidents.
- Incidents are investigated by staff or School Leadership, with the following details being recorded into SEQTA: A description of the incident, the incident/s date, time, students involved, teachers/staff, location and summary will be recorded.
- Incidents are referred to the School Leadership Team, IT Coordinator or Welfare Coordinators.
- The school Behaviour Policy and Student Behaviour guidelines will determine the action to take for breaches of the Student Owned Device User Agreement.
- Students may lose digital technology privileges for a designated length of time and may be required to complete reflections and activities surrounding restorative practices.
- Parents will be notified and expected to meet with school staff if students are involved in incidents of bullying/cyberbullying as per Cyber-Bullying Procedure.
- Notification will be given/sent to leadership when breaches occur.
- In the case that an online activity is illegal, then as such it will be reported to police. These records are stored in SEQTA and details can be accessed by authorised school staff.



Implementation

- All members of the school community should be aware of and have knowledge of the documents listed above.
- All teachers must discuss/teach the content of the Acceptable Use Agreement in Term One of each year and classroom Digital Technology rules at the beginning of each term.
- All students in years 3-12 must sign a copy of the Student Owned Device User Agreement and the eLearning and Technology Procedure annually.
- A copy of all the Policies, including the eSmart Policy, Student Owned Device User Agreement and the eLearning and Technology Procedure are displayed on the school website.
- Any breach of the Acceptable User Agreement is recorded on SEQTA.
- Parents will be notified of any User Agreement breaches.
- Parents, teachers, students and the community will be aware of the school's position on cyber bullying.
- Teacher will be regularly reminded of their duty of care regarding protection of students from all forms of bullying.
- The school community will be updated on a regular basis through newsletters, fact sheets, information sessions, the school's Facebook page and the school website.
- Australian Curriculum Digital Technologies Curriculum will be explicitly taught and supported in classrooms.
- Incidents and complaints process will be made clear to students and parents.
- New students and staff will be informed at the start of the start of the school year, or upon the time of entry into the school.

CYBER BULLYING PREVENTION (As per the schools Cyber-bullying procedure)

A. Primary Prevention

- Professional development for staff relating to all forms of bullying including cyber bullying. Harassment and proven counter measures.
- Educate the school community about the seriousness of cyber bullying, its impact on those being bullied and how this behaviour is unacceptable.
- Provide programs that promote resilience, life and social skill, assertiveness, conflict resolution and problem solving.
- Each classroom teacher to clarify with students at the start of each year the school policy on bullying, including cyber-bullying.
- All students to be provided with individual and confidential computer and network log ins and passwords. Processes to be put in place to ensure tracking of student activity on the school's computer equipment and network. Firewalls to be installed to eliminate outside traffic into the school's network and intranet.
- The use of mobile phones by students will be limited with consequences to implement for any students who use mobile phones inappropriately.
- The curriculum to include anti-bullying messages and strategies eg: 'Think You Know' and 'Values' programs.
- Student Representative Council, Staff and Students to promote the philosophy of 'Positive Behaviour for Learning'



B. Early Intervention:

- Encourage children and staff to report bullying incidents involving themselves or others.
- Classroom teachers and principal on a regular basis reminding students and staff to report incidents of bullying.
- Regular monitoring of student traffic on school's computer networks to identify potential problems.
- Parents encouraged to contact school if they become aware of a problem.

C. Intervention:

- Once identified each bully, victim and witnesses will be spoken with, and all incidents or allegations of bullying will be fully investigated and documented.
- Parents to be contacted.
- Students and staff identified by others as bullied will be informed of allegations
- Both bullies and victims will be offered counselling and support.
- Removal of cyber bullies from access to the school's network and computers for a period of time.
- Loss of privilege to bring a mobile phone to school for students who bully via SMS or similar telephone functions.
- If student bullying persists parents will be contacted and consequences implemented consistent with the school's Student Code of Conduct and Student Behaviour Management Policy.

D. Post Violation:

Consequences for students will be individually based and may involve:

- Exclusion from class.
- Exclusion from playground.
- School suspension.
- Withdrawal of privileges.
- Ongoing counselling from appropriate agency for both victim and bully.
- Reinforcement of positive behaviours.
- Support Structures put into place to support positive behaviour choices
- Ongoing monitoring of identified bullies.
- Positive behaviour tracking

Review date: 21/11/17

Evaluation:

Ratified by Heritage College School Council February 2017