eSmart Cyber Safety Policy

Vermont Primary School

Vermont Primary School (VPS) recognises the importance of Information and Communications Technologies (ICT) in preparing students for the world around them. VPS acknowledges that the effective and safe use of technology relies upon the development of responsible cyber-citizenship, and is committed to being an eSmart school. VPS believe that explicitly teaching students about safe and responsible online behaviours is essential, and is best taught when linked to the school's values - RESPONSIBILITY, RESPECT, CARING & STRIVE and in partnership with parents/guardians. To be safe online and to gain the greatest benefit from the opportunities provided through an online environment, students need to follow the Vermont Primary School Acceptable Use Agreement developed in conjunction with students at our school. Safe and responsible behaviour is explicitly taught at our school and we request that parents/carers discuss and reinforce this behaviour at home.

Guidelines

Vermont PS is an accredited Alannah and Madeline Foundation eSmart School and works actively to maintain accreditation using the eSmart System Tool.

Implementation

School Practices

- Vermont PS supports the smart, safe and responsible use of digital technologies
- The Student Engagement and Wellbeing Policy, Student Code of Conduct and Internet and Digital Hardware Policy are in place ~~that~~ and clearly outline~~s~~ the values and expected behaviours of the school
- The Student Engagement and Wellbeing, Student Code of Conduct and Internet and Digital Hardware Policies are in place and clearly outline the values and expected behaviours of the school
- Use a secure internet based 'cloud' service to store and share student work that is approved by the Department of Education
- During Digital Technologies all students to be made aware of the Internet and Digital Hardware Policy for school practices that aim to keep students safe at Vermont PS (Acceptable Use Agreements)
- All staff to read the Internet and Digital Hardware Policy for school practices that aim to keep students safe at Vermont PS

- Students' full names are never to be placed in an online environment, students will only be referred to by their first name and last initial
- Images of students will only be uploaded where parental permission has been obtained

Use Agreements

- Students and parents/guardians will be required to sign the Student Internet Use Agreement before students are permitted to access the school network, internet and ICT resources. These will be re-issued annually to ensure students and parents are aware of their responsibilities (see Internet and Digital Hardware Policy)
- A copy of the Student Internet Use Agreement will be displayed in all classrooms

Education

Whole School

- The Engagement and Wellbeing Team will provide the school community with education regarding cyber safety on a regular basis through the school Newsletter
- Cyber safety will be regularly promoted to the school community through school newsletters, presentations at assembly and information sessions
- The Cyber Safety Program is reinforced across the whole school led by the Engagement and Wellbeing Professional Learning Team
    - It is the responsibility of all staff at Vermont Primary School to promote and educate the students to become safe digital citizens
    - In addition to this the Digital Technologies Specialist Teacher implements the Vermont PS Cyber Safety Scope and Sequence (Appendix A)

Students

- Students are explicitly taught Cyber Safety skills and strategies through the Digital Technologies Specialist Subject and their classroom teacher
- Students are educated about the Student Code of Conduct, Engagement and Wellbeing Policy and the Acceptable Use Agreements at the beginning of each school year, or once enrolled at Vermont PS
- Students in Years 3 to 6 will follow the **eSmart CPR** acronym
    - **Communicate -** I will **communicate respectfully** by
        - ✓ stopping and thinking to check that what I write or post is polite and respectful
        - ✓ being kind to my friends and classmates and thinking about how the things I do or say online might make them think or feel
        - ✓ working to stop bullying. I don't send mean or bullying messages or pass them on to others
    - **Protect -** I will **protect personal information** by:
        - ✓ being aware that my full name, photo, birthday, address and phone number is personal information and is not to be shared online
        - ✓ protecting my friends' information in the same way
        - ✓ protecting my passwords and not sharing them with anyone except my parents
        - ✓ only ever joining online spaces with my parents or teacher's guidance and permission
        - ✓ never answering questions online that ask for my personal information
    - **Respect -** I will **respect myself and others** by thinking about my actions:
        - ✓ use spaces or sites that are appropriate for my age and if I am not sure I ask a trusted adult for help
        - ✓ speak to a trusted adult if I see something that makes me feel upset or if I need help
        - ✓ speak to a trusted adult if someone is unkind to me or if I know someone else is upset or scared

- ✓ don’t deliberately search for something rude or violent
- ✓ turn off the monitor if I see something I don’t like and tell a trusted adult
- ✓ create and present my own work and if I do copy something from the internet, letting others know by sharing the website link to acknowledge the creator
- ✓ being careful with the equipment I use

- Students in Years Foundation to 2 will follow the THINK acronym:
  - **Tell Someone**
    - ✓ Tell a trusted adult (Mum, Dad, teacher) if you see something that upsets you or if someone online makes you unhappy
  - **Hide your password**
    - ✓ Only tell your Mum, Dad or trusted teacher
    - ✓ If someone else asks me what my password is, do not tell them
  - **Interesting websites**
    - ✓ Interesting websites can be fun. Ask Mum or Dad if a site is ok to use
    - ✓ Only use websites that are appropriate for my age
    - ✓ Only use the internet when a teacher is with me in the classroom
    - ✓ Only use the internet to complete work set by my teacher
    - ✓ Turn the monitor off if I see something that makes me feel uncomfortable and tell the teacher
  - **Name calling**
    - ✓ Name calling or being mean online is not cool – we call it Cyberbullying
    - ✓ Be nice when communicating online
    - ✓ Look out for yourself and others
    - ✓ Speak to a trusted adult if someone is unkind to me or my friends
  - **Keep your personal information safe**
    - ✓ Don’t give your real name, address or phone number to anyone you don’t know in the real world
    - ✓ Use a nickname online

Parents

- Parents are encouraged to support the school in encouraging responsible communication using ICT equipment/devices at school and at home
- Parents are asked to discuss the Acceptable Use Agreement with their child/children and explain why it is important
- Support the school’s cyber-safety program by emphasising to their child the need to follow cyber-safety strategies and sign the Use Agreement,
- Contact the Engagement and Wellbeing Leader or a teacher to discuss any questions or concerns they may have about cyber-safety and/or the Use Agreement.

Teachers

- Teachers will plan and implement cyber safety lessons that outline the User Agreement and Breaches of the Agreement
- Cyber safety will continue to be reinforced and taught throughout the year by the classroom teacher
- Teachers will ensure new students and their parents understand the school's Acceptable Use Agreement and will teach new students the school's values.
- The Engagement and Wellbeing Leader will ensure new staff are aware of the school's practices and procedures in all areas of cyber safety
- All teachers must report any cyber incidences or breaches of the User Agreement to the Engagement and Wellbeing Leader and follow the whole school procedures (Appendix B and C)

<u>Breaches to the User Agreement and Cyber Incidents Reporting</u>

- Parents/guardians will be notified and expected to meet with relevant school staff if their child is involved in any incidents of cyberbullying or breaches of the User Agreement
- All staff must follow the Vermont PS Responding to Cyber Incidents Procedures (Appendix B and C) when responding to a report
- The Engagement and Wellbeing Leader collects and monitors data relating to incidents
    - Vermont Primary School will provide an anonymous means of reporting Cyber Incidents on the school website
        - Information on when to use this procedure will be made available to the school community via the newsletter and to the students via the classroom teacher
        - The monitoring of the reported incidents is completed by the Engagement and Wellbeing leader

This Policy works in conjunction with:

1. VPS Child Safety Policy
2. VPS Child Safety Code of Conduct
3. Wellbeing and Engagement Policy
4. Bullying and Harassment Policy
5. The Student Code of Conduct

Evaluation

The Policy Sub Committee and Vermont Primary School staff will review the effectiveness of the school's E-Smart Policy on a cyclical basis in accordance with DET guidelines.

APPENDIX A - eSmart Scope and Sequence - Foundation - 2

	Foundation	1	2
Internet Safety	Internet – everyone can access, if you see something safe – what can you do	THINK – teach the acronym Going Place Safely – Commonsense Media Lesson 1 Staying Safe Online Commonsense Media	THINK – teach the acronym
Privacy & Security	Username & password and they're private Dots instead of letters for passwords Only go into your folder Hector's world Personal Information: Episode 1- "Details, Details, Details"	Hector's world We need to protect our private information Episode 2- "Welcome to the Carnival"	Hector's world Do we know what we are signing up for? Episode 3- "It's a Serious Game" Episode 4- "The Info Gang" Episode 5- "Heroes"
Online Behaviour & Friendships	Modelling respectful online behaviours and addressing any concerns that arise	THINK – teach the acronym	Dippy Duck's Big Decision Students learn the importance of what not to post Screen out the Mean Defines Cyberfullying *Commonsense Media*
Creative Credit & Copyright	Concept of having ownership over your work – name & date etc Copy photos from the Internet and write where we got them from.	My Creative Work Having ownership over work & giving credit Commonsense Media	
Digital Footprint and Reputation	Avatars	Follow the Digital Trail Students learn that the information they put online leaves a digital footprint or "trail." This trail can be big or small, helpful or hurtful, depending on how they manage it.	Links to Dippy Ducks Big Decision
Information Literacy			Using Key Words Students understand that keyword searching is an effective way to locate information on the InternetStudents examine their search results and observe how a good choice of keywords can get them the information they want. Sites I Like Students explore and evaluate an

			informational website for children. Students discover that people's opinions about the quality and usefulness of a site will vary.

eSmart Scope and Sequence – 3-6

	3	4	5	6
Internet Safety	Comic Book Capers Interactive quiz on internet safety	Budd:e Covers a variety of internet safety, security & privacy topics	Digital Passport Commonsense Media How Cybersmart are You? Online quiz on cyber safety	Digital Licence eSmart program covering a wide range of topics
Privacy & Security	Lee and Kim Watch clip about privacy in online games & relate back to THINK & Internet Use agreement Private & Personal Information How can you protect yourself from online identify theft? Students think critically about the information they share online. Commonsense Education	Rings of responsibility Students explore what it means to be responsible to and respectful of their online and online communities as a way to learn how to be good digital citizens. Use Publisher to create the rings. Commonsense Education	Strong Passwords Students learn how to create secure passwords in order to protect their private information and accounts online. Commonsense Education	Scams & Schemes Students learn strategies for guarding against identity theft and scams that try to access their private information online. Commonsense Education
Online Behaviour & Friendships	Show Respect Online Students explore the similarities and differences between in-person and online communications, and then learn how to write clear and respectful messages. Commonsense Education	Using Technology in the Classroom Collaborate as a class to establish an agreed set of behaviours when using technology. (eSafety website) Balancing Your Time Online How much is too much? (eSafety website)	Jigsaw video This video looks at privacy in social media and potential consequences. Discuss ways to report at school and home.	Cyber bullying Bullystoppers interative module and activity guide
Creative Credit & Copyright		Whose Is It Anyway? Students learn the copying the work of others and presenting it as ones' own is called plagiarism. They also learn about when and how it's ok to use the work of others. Commonsense Education	Picture Perfect Students learn how photos can be altered digitally. They will consider the creative upsides of photo alterations as well as its power to distort our perceptions of beauty and health Commonsense Education	A Creators Rights Students are introduced to copyright, fair use and the rights they have as creators. Commonsense Education
Digital Footprint and Reputation	The Power of Words Students consider that they may get online messages from other kids that can make them feel angry, hurt, sad or fearful. Students identify actions that will make them Upstanders in the face of Cyberbullying. Commonsense Education	Covered in the Budd:e program	Covered in Digital passport	Social Media Bullystoppers interactive module & activity guide
Information Literacy	The Key to Keywords Students learn strategies to increase the accuracy of their keyword searches and	How to Cite a Site Students reflect on the importance of citing all sources when they do research.	Strategic Searching Students learn that to conduct effective and efficient online searches, they must	Identifying High Quality Sites Students learn that anyone can publish on the Web, so not all sites are equally

	make inferences about the effectiveness of the strategies. Commonsense Education	They then learn how to write bibliographical citations for online sources. Commonsense Education	use a variety of searching strategies. Commonsense Education	trustworth.

APPENDIX B

VPS Staff Procedure for Responding to Moderate Cyber Incidents Affecting Students

Step 1	Step 2	Step 3	Step 4	Step 5
Identify Concern	**Take Action**	**Respond**	**Consequences**	**Record**
Talk to and discuss the incident with all parties , if it is one of the scenarios below proceed with this flow chart. If not turn over to the Severe Incident flow chart. If unsure see Julie Hall or Helen Murphy ⇒ Making general negative comments online ⇒ Plagiarism ⇒ Using or sharing Passwords ⇒ Inappropriate language online ⇒ Searching for content that is inappropriate or illegal ⇒ Posting our own personal information online (see AUA) ⇒ Having 'underage' social media accounts	Ensure all students are safe Record details from all involved – this may include all staff and students who may have been directly or indirectly involved in the incident and/or its effects Keep any evidence – eg. screenshots, emails, texts etc	Refer to the relevant Acceptable Use Agreement and discuss how the 'incident' is a breach of this Contact Parents of all students (including witnesses in a manner that suits in the incident.)	Write, explaining how they have breached the eSmart CPR or THINK and what its impact was on others Warning for first time or unintentional offence OR Restricted use of technology for a short period of time Education targeted at year level where appropriate	Fill out a Cyber Incident report in Sentral Make sure to record the steps taken to resolve the incident eg. steps taken to remove content, mediation attempts Notify classroom teacher eSmart

APPENDIX C

VPS Staff Procedure for Responding to Severe Cyber Incidents Affecting Students

Step 1	Step 2	Step 3	Step 4	Step 5
Identify Concern	**Take Action**	**Respond**	**Consequences**	**Record**
Talk to and discuss the incident with all parties , if it is one of the scenarios below proceed with this flow chart. If not turn over to the Medium Incident flow chart. If unsure see Julie Hall or Helen Murphy ⇒ Damaging ICT Equipment ⇒ Making negative comments online targeting an individual or specific group ⇒ Identity Theft ⇒ Stealing passwords or using another individual's password for inappropriate or malicious use ⇒ Work or images that personally attack, humiliate or defame an individual ⇒ Posting other people's personal information online (see AUA) ⇒ Accessing and/or meddling with the school network	Ensure all students are safe Record details from all involved – this may include all staff and students who may have been directly or indirectly involved in the incident and/or its effects Keep any evidence – eg. screenshots, emails, texts etc If the incident is found to be a criminal act, notify Parents and police ASAP after consulting executive team.	Provide reasonable & ongoing wellbeing support to all students & staff who were involved in or witness to the event Refer to the relevant Acceptable Use Agreement and discuss how the 'incident' is a breach of this Where relevant work with families, social media/game/messaging sites to take down inappropriate/offensive material Contact Parents of all students, including witnesses	Write, explaining how they have breached the eSmart CPR or THINK and what its impact was on others Warning for first time or unintentional offence OR Restricted use of technology for a short period of time Education targeted at year level where appropriate	Fill out a Cyber Incident report in Sentral Make sure to record the steps taken to resolve the incident eg. steps taken to remove content, mediation attempts Notify classroom teacher Notify student welfare co-ordinator eSmart

Ra ue for

Ratified by School Council June 2018

Due for Review 2022