MALVERN VALLEY PRIMARY SCHOOL

CYBER SAFETY POLICY

WELLBEING

RATIONALE:

Technologies, the Internet, Social Media and Applications provide students with unprecedented opportunities to obtain information, engage in discussion, and liaise with individuals, organisation and groups world-wide so as to increase skills, knowledge and abilities. The implementation of specific cyber safety initiatives at Malvern Valley Primary School supports the safety and wellbeing of students and contributes to the prevention of unacceptable behaviour via technology, including cyber-bullying.

AIMS:

- To ensure that technology is used in the most productive way to enhance learning opportunities, whilst maintaining a focus on student or teacher wellbeing.
- To utilise the eSmart accreditation framework to provide a safe and supportive environment for students to utilise the Internet for their learning.
- For students to develop skills on how to use the technology appropriately and their responsibility as users of the Internet through initiatives included in the school curriculum
- To ensure the school has clear protocols for the use of technology
- To foster a consistent and integrated approach between the school values, behaviour management procedures and cyber use.
- To ensure the school provides learning opportunities for staff and parents about cyber safety
- To reinforce the importance of the school and parents working collaboratively to ensure cyber safety

IMPLEMENTATION:

The provision of a safe and educative cyber-safety community requires a multi-faceted implementation process. The school will utilise the framework for accreditation from the eSmart program to guide its implementation and ensure it is both comprehensive and relevant. The Assistant Principal and eSmart Coordinator will be responsible for ensuring the maintenance of accreditation standards. The implementation process of a cyber-smart school includes the following facets.

Protocols for the Use of Digital Technologies

1.1 The school requires all parents to read through and explain the agreement with their child(ren) and sign with them (junior years to have parent / guardian sign only) the 'Digital Technologies Acceptable Use Agreement' before they are able to use any digital technology devices.

1.2 Students will be supervised whilst using any digital technologies at school; teachers should always be able to see screens.

1.3 Students will not be permitted to use digital technologies during wet/hot day timetables (excepting projectors for classes watching programs)

1.4 All students will have censorship filtered Internet at school.

1.5 All Grade 3-6 students have their own password-protected (using automatically generated passwords) account to log on to school computers. Junior students will log on using class accounts. Their use on these accounts can be monitored/tracked by the school Information and Communication Technologies (ICT) Technician.

1.6 Students are required to sign in and leave any mobile devices at the office for the duration of the school day

1.7 The school will ensure that appropriate processes for dealing with incidences of cyber-bullying are documented in the Student Engagement and Inclusion Policy and Bullying Prevention Policy.

Student Education / Curriculum Framework

2.1 A whole-school approach to the education of students' responsible use of digital technologies will be implemented. The ICT/eSmart Committee will be responsible for disseminating initiatives and resources.
2.2 All teachers will explicitly teach cyber safety a minimum of 10 hours per year; however, (authentic) references to cyber safety will be embedded in curriculum.
2.3 The school's values of respect, friendliness, confidence, tolerance, cooperation and resilience will underpin all cyber education programs and will be explicitly referred to, enabling students to make connections.
2.4 The Technologies Learning Area of the Victorian Curriculum will be taught and assessed in accordance with DET requirements.
2.5 Teachers will utilise a variety of resources to educate students on age appropriate cyber safety issues including: digital footprint, privacy, stranger danger, plagiarising, cyber-bullying social media, information sharing and appropriate content. Resources that staff may use include, but are not limited to:
- http://www.cybersmart.gov.au/
- http://www.cybersmart.gov.au/young%20kids/visit-hectors-world.aspx
- http://www.bullyingnoway.gov.au/
- http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/what.aspx
- www.edmodo.com
- www.kidshelp.com.au

2.6 In accordance with the school's Bullying Prevention Policy, students will be educated on the importance of bystanders in minimising harm with regard to cyber-bullying.

Learning Opportunities for School Staff and Parents

3.1 All staff will be made aware of the requirements for educating students (including minimum eSmart accreditation requirements) and supported in the development of any skills and/or knowledge necessary to effectively teach cyber safety in their classroom.
3.2 Interactive Learning Modules will be utilised in staff meetings to ensure staff are up to date with the latest information and 'digital trends' and know how best to deal with situations that arise. Examples of modules to be used are:
- http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/bullystopmodules.aspx
- http://tplm.safeschoolshub.edu.au/Login/ for PL as well

3.3 All new staff will be inducted as to the requirements of teaching cyber safety and the related policies and processes as a part of their staff induction training.
3.4 New families to the school will receive a copy of the 'Digital Technologies Acceptable Use Agreement' upon their enrolment and will be required to complete it before students use digital technologies.
3.5 Information on the school's strategies and policies will be communicated to parents in newsletters, on the shool's website and available in the Policy Folder at the Office.
3.6 Relevant information, such as 'Parenting Ideas' and eSMART articles will be placed in the school newsletter and on the school's website for parents to read.

Incident Reporting and Guidelines

4.1 Teachers will ensure that students understand their responsibility for notifying an adult of any inappropriate material (online or in Applications) so that access can be blocked.
4.2 All staff shall be responsible for notifying the ICT technician of any inappropriate material so that access can be blocked.
4.3 In the same way that students are expected to notify a teacher of a bullying incident, students will also have a responsibility to raise concerns with a teacher and/or trusted adult if they are aware of any cyber-bullying.
4.4 In situations of cyber-bullying, whether at school our out of school, staff will follow the procedures (both in the intervention and post-incident) outlined in the school's Bullying Prevention Policy. If the incident is only occurring out of school, it will ultimately be the responsibility of the involved students' parents to monitor student cyber activity.
4.5 In situations of cyber-bullying where the behaviour is continuing to occur outside school hours, staff will provide access to educative resources for parents and students (where appropriate) focusing on the responsible use of digital technologies.

4.6 Communication with parents in instances of cyber-bullying will be thorough, ongoing and documented on Sentral.

Community Responsibility and Links

5.1 An eSmart Committee will communicate to ensure that the community has an active voice in the implementation of cyber safety within the Malvern Valley Primary School community.

5.2 In the formation of the Cyber Safety, Bullying Prevention and Student Engagement and Inclusion Policies (all of which play a significant role in the cyber safe practices of the school), input from members of the parent community will be sought.

5.3 Parents will be reminded at all school events not to post photos of other students online or to social media platforms.

EVALUATION:

This policy will be reviewed with whole staff, student, parent and community input as part of the school's three-year review cycle.

REFERENCE:

- ICT Acceptable Use Agreement
- Bullying Prevention Policy
- Student Engagement and Inclusion Policy
- https://www.esmartschools.org.au
- https://www.esafety.gov.au/esafety-information/games-apps-and-social-networking/

Ratified by School Council: **2017**

To be reviewed: **2020**