



Rationale

We want our students to be confident and safe while using technology in our school. Diamond Creek Primary School will be an eSmart school and promote cyber safety in the community. We believe that explicitly teaching about safe and responsible online behaviours is essential, and we feel that involving families in this process will be crucial for the eSmart program's success. We hope that families will support this program by reinforcing good decision making and appropriate use of technology at home.

Definition

Cyber bullying is when a person is tormented, threatened, harassed, humiliated, embarrassed or targeted by another person using the Internet, mobile phone, instant messaging, email, chat rooms, chat apps, social networking sites such as, but not limited to, Facebook, Twitter Instagram, Kik, or other types of digital technology.

Implementation

All students will undertake a Cybersafe program at school under the guidance of teachers. Before being allowed to use school computers all students must sign an Acceptable Use Agreement (Appendix 1), outlining expectations and standards of behaviour for the use of technology at school. The school community will be provided with information on being Cyber Safe on a regular basis, through parent information sessions, newsletter articles and information from other sources. Incidents of Cyber bullying will not be tolerated at Diamond Creek Primary School. Victims and their carers will be encouraged to report incidents occurring outside of school hours to law enforcement bodies. Any incidents that occur during school hours will be dealt with in consultation with the eSmart committee, Principal and families of students involved in accordance with this policy.

Code of Conduct Agreement

Under the supervision of teachers, students are responsible for appropriate behaviour on the school's digital learning network. Students and their parents are asked to sign an agreement on digital learning usage prior to the student being allowed to access the Internet at school. This agreement aims to ensure that parents and students are aware of their responsibilities with regard to appropriate use of computers/ ICT equipment and understand the consequences of breaking these rules. Diamond Creek Primary School endeavours to be a Cyber Smart school and uses Cyber Safe guidelines when learning with technology.

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

- Withdrawal of access to the school network and devices
- Confiscation of personal devices that may have been used inappropriately
- Devices believed to contain evidence of a criminal act may be held and handed to Police for evidence
- Devices believed to have been used inappropriately may be held and collected by parents a time to be determined by the school Principal or eSmart committee members
- Suspension in cases of serious misconduct

It is a criminal offence to use an ICT device to menace, harass, make threats or offend another person. In these instances, the school may consider it

- appropriate to involve the Police.
- In investigating a suspected breach of this Policy the User agrees to promptly make

the ICT equipment/device available to the school for the purpose of any investigation and/or audit and to cooperate otherwise with the school in any investigation or audit process. The terms of this policy form part of the school's expectations for the purpose of a student's enrolment at Diamond Creek Primary School.

E-Smart User Obligations

1. eSmart Agreement

1.1 As the school provides network and internet access, the contents of the school's ICT system remains property of the school. The school 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.

1.2 All users, whether or not they make use of network facilities and communication technologies on school owned or personal ICT equipment/devices will have full access to this policy via the school web page: <http://www.diamondcreekps.vic.edu.au/>

1.3 The school's ICT equipment, including network facilities, communication technologies, eLearning tools and general ICT equipment/devices all fall under this policy. The use of personal ICT and communication devices, where necessary, fall under this policy if used at school.

2. Obligations and requirements regarding appropriate use of ICT in the School

2.1 While on school grounds, using school owned ICT equipment/devices is for educational purposes only.

2.2 When using school or private ICT equipment within school grounds, or relating to the members of the school community, inappropriate use may include but is not limited to:

- Things that might 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
- never authorised by the school, including persons within the school community and persons/ organisations outside the school 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
- Brings the school into ill repute
- Results in unauthorised external administration access to the school'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 school
- Involves malicious activity resulting in deliberate damage to school ICT and/or ICT equipment/ devices
- Involves the unauthorised installation and/or downloading of non-school endorsed software
- Breaches the ethos and values of the school (RESPECT for self, others, learning and the environment)

2.3 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 supervising teacher or school Principal

2.4 While at Diamond Creek Primary School or on excursions or camps, Users must not have involvement with any material which might place them at risk or breaches the ethos of the eSmart Policy. This includes images or material stored on privately owned ICT equipment/devices brought onto School property.

2.5 Users must not attempt to download, install or connect unauthorised software or hardware onto school ICT equipment, or utilise such software or hardware. This includes use of such

technologies as Bluetooth, infrared and wireless, and any other similar technologies that are available.

3. Monitoring by the School

The School:

- 3.1 Reserves the right at any time to check work or data on the school's computer network, email, Internet, computers and other school ICT equipment/devices, without obtaining prior consent from the relevant User.
- 3.2 Reserves the right at any time to check work or data on privately owned ICT equipment on the school grounds or at school related activities. The User agrees to promptly make the ICT equipment/device available to the school for purposes of any such check and to otherwise co-operate with the school in the process. Before commencing the check, the school will inform the User of the purpose of the check.
- 3.3 Has an electronic access monitoring system, 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.
- 3.4 Monitors traffic and material sent and received using the school's ICT infrastructures. From time to time this may be analysed and monitored to help maintain an eSmart learning environment.

4. Copyright, Licensing, and Publication

- Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos and images.
- All material submitted for internal publication must be appropriate to the school environment and copyright laws.
- Materials submitted for publication of the school facebook page can only be done so with permission of the parents, students and teachers.
- Material published on the school facebook page must be in line with the ethos and values of the school (RESPECT for self, others, learning and the environment).

5. Individual password logons to user accounts

- 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.
- Authorised users must not allow another person access to any equipment/device logged in under their own user account. Material access on a user account is the responsibility of that user. Any inappropriate or illegal use of the computer facilities and other school ICT equipment/devices can be traced by means of this login information.
- Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Policy. This includes ensuring that no electronic communications could cause offence to other 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 school environment.
- For personal safety and having regard for 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.

6. Privacy

- The Privacy Act requires the school take reasonable steps to protect the personal information that is held by on its systems from misuse and unauthorised access. Users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.
- While after school use of communication technologies by students is the responsibility of parents, school policy requires that no student attending the school may identify, discuss, photograph or otherwise publish personal information or personal opinions about school staff, fellow students or the school. Any such behaviour that impacts negatively on the high public standing of the school may result in disciplinary action. The school takes a strong position

7. Procedures for Mobile Phone Use at School

- The school accepts that some parents provide their children with mobile phones to protect them from everyday risks involving personal security and safety. Use of mobile phones during school hours is prohibited, and all mobile phones brought to school must be checked in at the school office to be stored in the strong room for the duration of the school day. Students are expected to drop their phones at the office as soon as they enter the school grounds and pick them up at the conclusion of the school day. Phones are not to be used in the school yard, even prior to the school bell, and only for contact with families organising to pick up their students at the conclusion of the school day following the bell.
- Any student found to be in possession of a mobile phone during school hours can expect to have the phone confiscated, to be collected from the Office or Principal after school.
- Parents wishing to contact their student during school hours must do so through the appropriate channel of ringing the school office on 9438 1108.
- Mobile phones brought to school are the sole responsibility of the student and no liability for lost, stolen or misplaced phones is accepted by the school. Once handed in at the office mobile phones will be stored in the office, with every care taken to ensure their security.

8. When using a digital device such as a camera or iPad I will:

- Only take photos and record sound or video with the permission of the teacher.
- Seek permission from individuals involved before taking photos, recording sound or videoing them (including teachers).
- Seek written permission from the Principal or Classroom Teacher before publishing any image, sound or recording taken at Diamond Creek Primary School, related school events or of students in Diamond Creek Primary School uniform.
- Be respectful in the photos or video I take and never use these as a tool for bullying.

How else can parents assist?

- Read and discuss the eSmart policy with your child
- Encourage your child to comply with the school's eSmart Policy
- Ensure your child takes full responsibility for the proper use, storage and liability of ICT/ Communications products brought onto school grounds
- Support the school in the enforcement of the eSmart Policy
- Follow procedures and protocols detailed above in relation to acceptable use of social media and technology where the school is involved. This includes seeking permission before posting any photographs of staff, students or parents and being mindful of not breaching the ethos and values of the school (RESPECT for self, others, learning and the environment)

EVALUATION

This policy will be reviewed regularly as part of the school's cyclic review process (every five years or sooner if required).