

Digital Technologies (Internet, social media and digital devices)

CONTEXT

This policy applies to all students and staff at the Donburn Primary School.

Staff use of technology is also governed by the Department's *Acceptable Use Policy*. The reference to the policy can currently be found on the Department of Education website: (www.education.vic.gov.au/school/principals/infrastructure/pages/acceptableuse.aspx

This policy also applies to use of digital technologies by all Donburn employees, contractors, students and the school community when representing Donburn in social media, or discussing Donburn or education related issues in their personal use of social media; this policy does not apply to your personal use of social media platforms, as long as you make no reference to Donburn

AIM

To ensure that all students and members of our school community understand:

- (a) our commitment to providing students with the opportunity to benefit from digital technologies to support and enhance learning and development at school.
- (b) expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops, tablets)
- (c) the school's commitment to promoting safe, responsible and discerning use of digital technologies, and educating students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and digital technologies
- (d) our school's policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet

POLICY

Vision for digital technology at Donburn Primary School

Donburn Primary School is committed to pursuing further enhancement of the children's learning with the use of digital technologies and systems.

Donburn Primary School understands that digital technologies including the internet, apps, computers and tablets provide students with rich opportunities to support learning and development in a range of ways.

Through increased access to digital technologies, students can benefit from enhanced learning that is interactive, collaborative, personalised and engaging. Digital technologies enable our students to interact with and create high quality content, resources and tools. It also enables personalised learning tailored to students' particular needs and interests and



transforms assessment, reporting and feedback, driving new forms of collaboration and communication.

Donburn Primary School believes that the use of digital technologies at school allows the development of valuable skills and knowledge and prepares students to thrive in our globalised and inter-connected world. Our school's vision is to empower students to use digital technologies to reach their personal best and fully equip them to contribute positively to society as happy, healthy young adults.

Safe and appropriate use of digital technologies

Digital technology, if not used appropriately, may present risks to users' safety or wellbeing. At Donburn Primary School, we are committed to educating all students to be safe, responsible and discerning in the use of digital technologies, equipping them with skills and knowledge to navigate the digital age.

Donburn Primary School:

- uses online sites and digital tools that support students' learning, and focus our use of digital technologies on being learning-centred.
- restricts the use of digital technologies in the classroom to specific uses with targeted educational or developmental aims.
- supervises and support students using digital technologies in the classroom.
- effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students.
- has programs in place to educate our students to be promoting safe, responsible and discerning use of digital technologies, including eSmart.
- educates our students about digital issues such as online privacy, intellectual property and copyright, and the importance of maintaining their own privacy online.
- actively educates and remind students of our Student Engagement policy that outlines our School's values and expected student behaviour, including online behaviours.
- has an Acceptable Use Agreement outlining the expectations of students when using digital technology at school.
- uses clear protocols and procedures to protect students working in online spaces, which
 includes reviewing the safety and appropriateness of online tools and communities,
 removing offensive content at earliest opportunity.
- educates our students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and other digital technologies.
- provides a filtered internet service to block access to inappropriate content.
- refers suspected illegal online acts to the relevant law enforcement authority for investigation.



 supports parents and carers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home through regular updates in our newsletter and annual information sheets.

Distribution of school owned devices to students and personal student use of digital technologies at school will only be permitted where students and their parents/carers have completed a signed *Acceptable Use Agreement*.

It is the responsibility of all students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects an account has been used by another person, the account holder must notify [insert relevant role, i.e. classroom teacher, the administration] as appropriate, immediately.

To maintain the highest level of safety standards and control, all messages created, sent or retrieved on the school's network are the property of the school. The school reserves the right to access and monitor all messages and files on the computer system, as necessary and appropriate. Communications including text and images may be required to be disclosed to law enforcement and other third parties without the consent of the sender.

Student behavioural expectations

When using digital technologies, students are expected to behave in a way that is consistent with Donburn Primary School *Statement of Values, Student Wellbeing and Engagement* policy, and *Bullying Prevention* policy.

Each year, students and parents/carers are required to complete the eSmart User Agreement applicable to each year level. Students will only be permitted to access digital technologies at school after the relevant eSmart User Agreement has been duly completed and received by the school.

When a student acts in breach of the behaviour standards of our school community (including cyberbullying, using digital technologies to harass, threaten or intimidate, or viewing/posting/sharing of inappropriate or unlawful content), Donburn Primary School will institute a staged response, consistent with our policies and the Department's *Student Engagement and Inclusion Guidelines*.

Use of Social Media

Social media are computer-mediated technologies that allow individuals, companies, NGOs, governments, and other organizations to view, create and share information, ideas, career interests, and other forms of expression via virtual communities and networks. Behavioral expectations apply to the use of electronic and virtual networks.



1. Students are expected to:

- Only access the social media channels through the School's network if the access is facilitated and moderated by a teacher for class work.
- Have regard to the impact of all social media postings within the extended school community.
- Avoid making disparaging statements or opinions about the School, the administration of the School or members of staff on any social media channels.
- Avoid making disparaging statements about fellow students on social media channels.
- Not use social media channels to bully, offend, harass, intimidate, masquerade or deliberately exclude other students or staff, whether within or outside of school hours.
- Realise that any material published on the internet is permanent and may be copied, misused and distributed by others.
- Unauthorised use of images on social media platforms can constitute a breach of privacy unless express authorisation has been sought.
- Understand that the publication of photos and tagging can reveal information about themselves and others and their location.
- Be aware that by identifying themselves as Donburn Primary School students (such as images in school uniform) immediately creates an association with the School and may affect the public image of the School.

Students feeling unsafe or intimated through the effects of social media or seeing others being affected by or participating in inappropriate on-line behaviour should seek assistance from a teacher.

2. Staff are expected to:

- Have approval to represent Donburn in Social Media.
- Disclose that they are a Donburn employee or contractor and be clear about what their role and accountabilities are.
- Be respectful of all individuals and communities you interact with online and seek to conform to the cultural and behavioural norms.
- Disclose only publicly available information.
- Not disclose other people's personal information.
- Not post material that is obscene, defamatory, threatening, harassing, discriminatory or hateful to another person or entity.
- Respect copyright, privacy and other applicable laws when publishing on social media.



Cyber Bullying

Bullying in any form is unacceptable. Bullying that is carried out through an internet service, such as email, chat room, discussion group or instant messaging or through mobile phone technologies such as short messaging service (SMS) is cyber bullying.

Cyber bullying can be very destructive and will not be tolerated at any level, and serious consequences exist for students who choose to bully others.

Parents, teachers, students and the community are to be made aware of types of cyber bullying, and its social and legal ramifications. Teachers will be regularly reminded of their duty of care regarding protection of students from all forms of bullying.

Donburn Primary School will adopt a four-phase approach to cyber bullying:

Phase 1 – Primary Prevention: Strategies that will be employed:

- Professional development for staff relating to all forms of bullying including cyber bullying, harassment and proven counter measures.
- Teachers will be trained in cyber safety. Cyber safety awareness programs will be provided for parents and cyber safety will form part of each child's ICT curriculum.
- Education of the school community about the seriousness of cyber bullying, its impact on those being bullied, how cyber-bullying occurs and consequences of cyber-bullying.
- Community awareness and input relating to bullying (including cyber-bullying), its characteristics and the school's programs and response.
- Programs that promote inclusiveness, resilience, life and social skills, assertiveness, conflict resolution and problem solving will form an integral part of our curriculum. In particular, assertiveness training and bystander training that builds skills in children to challenge and/or report unacceptable behaviour will be central to our curriculum.
- A student bullying survey and yard survey will be administered and acted upon twice annually.
- Each classroom teacher to clarify with students at the start of each year the school policy on bullying, including cyber-bullying.
- All students will be provided with individual and confidential computer and network passwords. Processes are in place to ensure tracking of student activity on the school's computer equipment and network. Firewalls are installed to eliminate outside traffic into the school's network and intranet.
- The use of mobile phones by students at school will be limited with consequences to be implemented for any students who use mobile phones inappropriately.
- The curriculum to include anti-bulling messages and strategies e.g.: 'The Friendly Schools' and 'No Blame Approach to Bullying' programs.



- Student Representative Council, peer support delegates, staff and students to promote the philosophy of 'No Put Downs'.
- Electives and structured activities available to students at recess and lunch breaks.

Phase 2 – Intervention:

- All incidents or allegations of bullying will be fully investigated and documented.
- The school will reinforce with children the importance of appropriately reporting incidents of inappropriate behaviour involving themselves or others, and the imperative that staff respond appropriately and proportionally to each allegation consistent with the school's Student Code of Conduct Policy, including reporting and recording of the incident on our on-line behaviour tracker.
- Students and staff identified by others as cyber bullies will be informed of allegations.
- Parents are to be informed if their child is alleged to have been bullied or experienced inappropriate behaviour, or if their child appears to have behaved inappropriately or bullied someone else.
- Appropriate and proportional consequences may include a verbal apology, writing a letter of regret, completing a behaviour Incident booklet, attending SOS, loss of privileges etc.
- Public recognition and reward for positive behaviour and resolution of problems as appropriate.
- 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 Policy*.
- Consequences of repetitive or serious incidents may include criminal charges, suspension, expulsion, loss of privileges, counselling, conciliation or any other consequences consistent with the school's Student Code of Conduct Policy.

Phase 3 – Post Violation:

It is important that appropriate strategies are put in place after bullying incidents have been resolved for all students involved. Appropriate strategies may include:

- Ongoing monitoring of students involved including network traffic.
- Identification of an agreed key contact staff member for each student involved.
- Follow-up meetings regarding each child's management strategy.
- Ongoing communication with parents.
- Counselling from appropriate agencies of support officers etc for both parties.



Reinforcement of positive behaviours and appropriate behaviour strategies.

Phase 4 – Evaluation:

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

Acceptable Use of Digital Technologies

The acceptable use of digital technology, equipment's, devices, computers and related resources by students is dependent on the acceptance by the student of the School's **eSmart Student User Agreement** as referenced in Annexure A and B.

In addition to the statements outlined in the agreement, the following principles apply:

- Students must follow all instructions from teachers when using school computers.
- Each student bears responsibility for their individual account. Students are not advised to share their account or password with any other student and must not access another person's account. At the end of each session, students should log out properly.
- Students must not reveal personal details about themselves or others, or arrange meetings, unless a teacher has given permission.
- Students are not permitted to post their email address or subscribe to content on a web page external to the School.
- Students must not send offensive email Send unsolicited email to multiple recipients (SPAM) Use email for any illegal, Immoral or unethical purpose.
- Students must not use their account to bully, offend or harass others. Harassment is defined as the persistent annoyance of another user or interference with another user's work.
- If students find or receive any information that is inappropriate or makes them feel uncomfortable, they should tell a teacher about it.
- Internet access is provided solely for educational use and school related activities only.
 Content filtering is used to prohibit access to inappropriate material. Deliberate attempts to locate or download material that is illegal or offensive are not permitted.
- Students must not tamper or interfere with or compromise any of the school's computer systems, cabling or peripheral equipment.
- Material such as games, sound, video or picture files (unless related to your schoolwork) must not be saved to the school network.
- Students should not use the network to access or send material which is racist, defamatory, obscene, pornographic or advocates violence or discrimination against other people.



- Students must not use the School's computer system to: download, install or distribute illegally copied software, games or music or change any computer settings.
- Eating or drinking is not permitted near any school owned computer resources.

The School will exercise due care with backups (if contractually responsible) but will not be held responsible for loss of data.

BREACH OF POLICY

Students and staff will be held responsible for their actions while using the school network. The misuse of ICT resources may result in the withdrawal of network access and disciplinary action.

Consequences for unacceptable behaviour including variances to this policy will be at the discretion of the Principal or his/her delegate.

They may include:

- removal of network access privileges
- removal of email privileges
- removal of internet access privileges
- removal of printing privileges
- other consequences as outlined in the school's Student Engagement and Welfare Policy and Student Welfare and Discipline Policy.

OTHER CONSIDERATIONS & RELATED DONBURN POLICIES

Donburn Primary School, Student Engagement and Welfare Policy Donburn Primary School, Student Welfare and Discipline Policy Donburn Primary School, Bullying Prevention and Management Policy Donburn eSmart Student User Agreement for Foundation to Grade 2 Donburn eSmart Student User Agreement for Grade 3 to Grade 6

DEFINITIONS

Term	Definition
Digital Technologies	Any networks, systems, software or hardware including electronic devices and applications which allow a user to access, receive, view, record, store, communicate, copy or send any information such as text, images, audio, or video.
ICT	Information and Communications Technology
DET	Department of Education and Training Victoria



Term	Definition
Cyber Bullying	Any direct verbal or indirect bullying behaviours using digital technologies. This includes harassment via a mobile phone, setting up a defamatory personal website or deliberately excluding someone from social networking spaces.
Bullying	An ongoing and deliberate misuse of power in relationships through repeated verbal, physical and/or social behaviour that intends to cause physical, social and/or psychological harm. It can involve an individual or a group misusing their power, or perceived power, over one or more persons who feel unable to stop it from happening. Bullying can happen in person or online, via various digital platforms and devices and it can be obvious (overt) or hidden (covert). Bullying behaviour is repeated, or has the potential to be repeated, over time (for example, through sharing of digital records). Bullying of any form or for any reason can have immediate, medium and long-term effects on those involved, including bystanders. Single incidents and conflict or fights between equals, whether in person or online, are not defined as bullying.

APPROVAL

Contact Person:	Policy Owner:
Principal	Donburn Primary School Council Education Sub Committee

DOCUMENT CONTROL

Version / Date Created	Nature of Amendment
Version 1 – Unknown	New Policy.
Version 2 – November	Merged the following Documents into this document
2016	IT – Acceptable IT Use 2103
Version 3 – August	Merged ICT & eSmart, Social media and Cyber Bullying policies,
2019	incorporated DET recommended template. Formatted and
	added information to required sections.

REFERENCES

Department of Education & Training, School Policy and Advisory Guide, *Using Social Media: A Guide for DET Employees*, Government of Victoria. Available from:

http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/socialmedia.aspx



[October 2016]

Department of Education & Training, School Policy and Advisory Guide, *Safe and Responsible Use of Digital Technologies*, Government of Victoria. Available from: www.education.vic.gov.au/school/teachers/support/Pages/safeandresponsibleuse.aspx [October 2016]

Australian Communications and Media Authority, *Information about how to filter digital content*, Government of Australia. Available from: www.acma.gov.au [October 2016]

Department of Education & Training, School Policy and Advisory Guide, *Acceptable Use Policy: DEECD Information, Communications and Technology Resources* (for staff), Government of Victoria. Available from:

http://www.education.vic.gov.au/Documents/school/principals/infrastructure/ictacceptableusepolicy.pdf [October 2016]

Department of Education & Training, School Policy and Advisory Guide, Acceptable use agreements and consent for students, Government of Victoria. Available from: http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/lolconsent.aspx [October 2016]

Department of Education & Training, School Policy and Advisory Guide, *Bullying Policy*, Government of Australia. Available from:

http://www.education.vic.gov.au/school/principals/spag/safety/pages/bullying.aspx [12 June 2015].

Department of Education & Training, School Policy and Advisory Guide, Cyber Teach Tool Kit - Safe and Responsible use of Digital Technologies, Government of Australia. Available from: http://www.education.vic.gov.au/about/programs/bullystoppers/Pages/cyberteach.aspx [12 June 2015]