

Bordertown Primary School

ICT & Cyber Safety Policy



Be honest – Practise bravery – Show kindness

Purpose

Bordertown Primary School provides students with access to ICT equipment/devices, the internet and other Information and Communication Technology (ICT) resources to support teaching and learning.

The purpose of this policy is to outline the school's approach to the safe, responsible and appropriate use of ICT equipment/devices and online technologies. The policy supports students to develop the knowledge, skills and behaviours required to use digital technologies safely, responsibly and respectfully.

Scope

This policy applies to all students in reception to year 6 when using school or department issued ICT equipment/devices, networks, internet services and digital platforms, whether these are accessed on or off school grounds.

Internet and access to ICT equipment/devices brings great benefits to the teaching and learning programs at Bordertown Primary School. All ICT equipment/devices are for educational purposes appropriate to a school environment, whether used on or off the site.

This policy includes information about Bordertown Primary School responsibilities, and the nature of possible consequences associated with ICT equipment/devices and cyber safety breaches that undermine the safety of the school environment.

Child protection education, such as the Keeping Safe: Child Protection Curriculum, includes information about remaining safe when using new technologies and is provided to all students. Our school also addresses online safety in our Good Start program at the beginning of each year.

More information about cyber safety can be found on Kids Helpline at <https://kidshelpline.com.au/> and on the safety website at <https://www.esafety.gov.au/kids>.

Parents and caregivers are encouraged to contact the school if they have any concerns regarding their child's safety when using ICT equipment/devices or online services.

Bordertown Primary School Responsibilities

Our responsibilities include:

- enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal, or harmful material on the internet or on ICT equipment/devices at school or at school-related activities.
- work with children and their families to encourage and develop an understanding of the importance of cyber safety through education designed to complement and support this policy. This includes providing children with strategies to keep themselves safe in a connected online world.
- respond to any breaches in an appropriate manner.
- welcome enquiries at any time from parents/caregivers or children about cyber safety issues.
- provide a filtered internet service to help restrict access to inappropriate, illegal or harmful material, while recognising that no filtering system can guarantee that all undesirable content will be blocked.
- monitor material sent and received through the school network and use filtering and/or monitoring software to restrict access to certain websites, data and email. Where electronic crime or serious incidents are suspected, the matter and any relevant devices may be referred to South Australia Police.



Bordertown Primary School

ICT & Cyber Safety Policy



Be honest – Practise bravery – Show kindness

ICT & Cyber Safety Expectations

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices regardless of the time of day. Being cyber safe is no exception and parents/caregivers must discuss with their child the following expectations to help them stay safe whenever they are using ICT.

1. Students must only use their own assigned device network accounts.
2. Students must not share personal information about themselves or other students with third parties, including their username or passwords. Personal information includes any of the following:
 - full name.
 - address.
 - e-mail address.
 - phone numbers.
 - photos of students and/or people close to them.
3. Students must not take photos or videos of another individual without their consent.
4. Personal information should not be entered onto websites that are not endorsed by the department, including writing aid, AI and chat websites (excluding EdChat).
5. Students must not engage in chats or other communication with third parties except when done so as part of curriculum learning.
6. AI software and websites should be used in an appropriate manner and not used for plagiarism or the creation of inappropriate or offensive content.
7. School ICT equipment/devices must not be used to access or share inappropriate content online, including sexually explicit materials, obscene depictions, harmful materials, illegal activities, profane or abusive language, or content that others may find offensive.
8. Web and email content filtering must not be circumvented to access content that has been deemed inappropriate for students.
9. Software designed to circumvent web and email content filtering or other security controls must not be installed or used on devices. This includes unapproved VPN software, proxy websites, hacking tools or the use of built-in device functions to bypass security controls.
10. Students must respect all school or department ICT equipment/devices and treat them with care. This includes:
 - not intentionally disrupting the running of any school ICT systems.
 - not attempting to hack or gain unauthorised access to any system.
 - following all school cyber safety expectations, and not joining in if other students choose to be irresponsible with ICT equipment/devices.
 - reporting any breakages/damage to a staff member.
11. Hacking, cheating and plagiarism tools must not be installed or used on devices. This includes software that gives users an unfair advantage in games or other activities.



Bordertown Primary School

ICT & Cyber Safety Policy



Be honest – Practise bravery – Show kindness

12. Copyright materials (including games, movies, photos, videos or programs) must not be illegally downloaded onto or accessed using school or department ICT equipment/devices.
13. When using online communities, users must communicate kindly and respectfully at all times. Students must not participate in harassing or bullying others online.
14. Students must comply with website terms of use, including age restrictions, appropriate access to the site and use of resources.
15. Students should not forward chain letters, spam or other unsolicited communications except to report these to ICT staff.
16. Students must not participate in business activities that are not staff approved or done so as part of curriculum learning.
17. Students must not violate any state or federal laws, including purchase of illegal items or substances, criminal activities punishable by law, etc.
18. Students should not use school or department ICT equipment/devices to stream or upload large volumes of data unless in the course of curriculum activities (e.g. streaming services such as Netflix, online gaming, livestreaming, etc).
19. Students must not connect unapproved hardware to any school or department network.
20. Students must not install unapproved software on school or department ICT equipment/devices.
21. Security software approved by the school should be installed on all devices connected to the school network or other department networks.
22. All students must report suspicious activity or violations of this policy to a staff member.
23. If students find anything that is upsetting, mean or rude, or know something is not acceptable at our school, they must:
 - turn off the screen.
 - not show others.
 - get a staff member straight away.
24. These policy expectations apply to any personal ICT equipment/devices brought to school.
25. If students do not follow these policy expectations, the school may inform their parents/caregivers. In serious cases, the school may take disciplinary action against students. Their family may be charged for repair costs. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.



Bordertown Primary School

ICT & Cyber Safety Policy



Be honest – Practise bravery – Show kindness

26. If students break the expectations of this ICT and Cyber Safety policy, the school will respond to incidents based on their nature and seriousness, in accordance with our:

- Behaviour Statement of Practice
- Anti-Bullying Policy
- Student Use of Phones & Other Personal Devices Policy

Students will not be able to use ICT equipment/devices at school until they change their approach to ICT use and their parents/caregivers have been contacted. The response may include temporary restriction or withdrawal of access to ICT equipment/devices, internet services or specific applications.

Policy review date: November 2028

DRAFT

