
SHELL COVE PUBLIC SCHOOL

Student Use of Digital Devices and Online Services Procedure

PURPOSE

This procedure guides student use of digital devices and online services at Shell Cove Public School.

Our school acknowledges the educational value of digital devices and online services in supporting and enhancing educational outcomes and student wellbeing. We also recognise they may cause harm if used inappropriately and that we need to support our students to use them in safe, responsible and respectful ways.

The Department of Education supplies Shell Cove Public School with computer devices, networks and other electronic information systems to meet learning goals, teaching practices and initiatives. These resources must be managed responsibly to maintain the confidentiality, integrity and availability of all information assets in compliance with the Department of Education Policy, Online Communication Services: acceptable usage for school students and the Professional Responsibilities Policy. These policies protect students, parents and staff against legal issues and damages.

SCOPE

This procedure provides a consistent framework for the safe, responsible and respectful use of digital devices and online services by students in our school. It sets out the shared responsibilities of school staff, students and parents and carers. It also provides a framework to manage potential risks to student safety and wellbeing.

This procedure covers student use of digital devices and online services in school-related settings, including on school grounds, at school-related activities and outside of school where there is a clear and close connection between the school and the conduct of students. This procedure covers the use of school-provided and personal digital devices and all online services.

All permanent employees, consultants, temporary and casual staff, students and members of the invited community must adhere to this policy. This policy applies to information assets owned or created by Shell Cove Public School, to devices that connect to Shell Cove Public School's network including third party providers and to devices which reside at the school site.

OUR SCHOOL'S APPROACH

Access to technology is vital in a future –focused learning environment to move our education system into a 21st century model of teaching and learning. Shell Cove Public School values the rich learning experiences that purposefully integrated technology brings. Staff, students and the community recognise the importance of students being equipped with the tools of 21st century learning. By facilitating a digital learning program, Shell Cove Public School empowers its students and gives them direct involvement in the way they use technology for learning.

This procedure establishes acceptable and unacceptable use of electronic devices and network services at Shell Cove Public School in conjunction with its established culture of ethical and lawful behaviour, openness, trust and equity.

Participants are responsible for exercising good judgment regarding appropriate use of resources in accordance with the Department of Education policies, standards, and guidelines. Shell Cove Public School's resources may not be used for any unlawful or prohibited purpose.

For security, compliance, and maintenance purposes, all staff must monitor and audit equipment, systems, and network traffic and communications as per the Code of Conduct. Devices that inappropriately interfere with the use of other devices or users on the Shell Cove Public School's network may be disconnected or prohibited according to the Student Wellbeing Policy.

System Accounts

Staff, students and members of the community are responsible for the security of data, accounts, passwords and systems under their control or supervision. These users must take appropriate measures to maintain security. They must keep passwords secure and not share account or password information with anyone, including other personnel, family or friends. They must deactivate systems which are no longer in active use and are not being monitored. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

Staff, students and members of the community must maintain system-level and user-level passwords in accordance with the Department of Education's Acceptable Use Policy.

All users must ensure through legal or technical means that proprietary information remains within the control of Shell Cove Public School at all times and all third party accounts used to communicate and educate students and the community must comply with the Department of Education's Social Media Policy and be developed in consultation with stage supervisors.

Students, staff and members of the community must:

- never knowingly initiate or forward emails or other messages containing:
 - a message that was sent to them in confidence.
 - a computer virus or attachment that is capable of damaging recipients' computers.
 - chain letters and hoax emails.
 - spam, e.g. unsolicited advertising material.
- never send or publish:
 - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
 - threatening, bullying or harassing material or messages,
 - sexually explicit or sexually suggestive material or correspondence.
 - false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and internet and online communication services are generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with Department business, is not permitted.
- never damage or disable computers, computer systems or networks of the department.
- ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling, personal social networking or any unlawful purpose.
- be aware that all use of internet and online communication services can be audited and traced to the accounts of specific users.

Bring your own device is an optional program where parents and carers can provide personal digital devices for use at school. All digital devices used in schools are covered by the *Student Use of Digital Devices and Online Services* policy. Schools retain discretion to determine the specifications of personal devices to be used at school.

Shell Cove Public School will restrict the use of digital devices to during class time. Use of devices at recess and at lunch must be approved by a teacher or Principal. Approval will only be granted for:

- an educational purpose;
- use of digital devices and online services as required for medical reasons;
- reasonable adjustments made as part of a student's individual education plan.

BYOD devices will be stored in classrooms during the school day.

Mobile Phones

If a student brings a mobile phone to school it must be handed to school office on arrival at school and collected from the school office at the end of the school day.

Should a student need to make a call during the school day, they should discuss this with their teacher, who will then organise this with the administration office.

During school hours, parents and carers are expected to only contact their children via the school office.

Assets

Staff, students and members of the community are responsible for ensuring the protection of assigned Shell Cove Public School assets (eg. Chromebooks, desktop computers/workstations, laptops and iPads). This includes the use of computer cables and third party attachments. Devices bought on site or left at Shell Cove Public School must be properly secured or placed in a locked drawer or cabinet. Any theft, loss or damage of assets must be promptly reported to the technology coordinator and/or administration staff.

All PCs, Chromebooks, iPads, laptops and workstations must be secured with a password activation. All users must lock the screen or log off when the device is unattended, staff must monitor and supervise this at all times.

Students, staff and members of the community connecting to Shell Cove Public School's network must read and agree to the Terms and Conditions shown upon login in accordance with the Acceptable Use Policy.

Staff, students and members of the community must not interfere with device management or security system software, including, but not limited to, antivirus, screensavers, filing systems and third party software.

Network Use

Staff, students and members of the community are responsible for the security and appropriate use of Shell Cove Public School's network resources under their control or supervision. Using Shell Cove Public School's resources for the following is strictly prohibited:

1. Causing a breach of security and/or policy to either Shell Cove Public School or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorised; circumventing user authentication on any device; or disabling network devices (eg: unplugging router from a port).
2. Causing a disruption of service to either Shell Cove Public School or other network resources, including, but not limited to, large downloads, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
3. Introducing honeypots, honeynets, or similar technology on the Shell Cove Public School's network.
4. Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.
5. Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws. See:
https://www.det.nsw.edu.au/policies/administrative/legal/screening_dvd/PD20060338.shtml
for additional information on export and transfer restrictions.
6. Use of the Internet or Shell Cove Public School's network that violates the Department of Education policies, or state and federal laws.
5. Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.
6. Port scanning or security scanning on a production network unless authorized in advance by the Department of Education.

CONSEQUENCES FOR INAPPROPRIATE USE

Staff

It is the responsibility of all employees to apply, promote and enforce the requirements of this policy in all interactions with technology related to their employment. Staff breaches of this policy, intentionally or otherwise, will be managed in accordance with the Department of Education Code of Conduct, in consultation with the staff member and school executive who will together review their technological practices.

Students and Community Members

Students and members of the community must behave in accordance with the requirements of this policy in all school related interactions with technology. Any student who is found to have breached these requirements will be subject to disciplinary action as outlined in the Shell Cove Public School Student Wellbeing Policy.

Students will be held responsible for their actions while using internet and online communication services. They will be held responsible for any breaches caused by them allowing any other person to use their accounts to access internet and online communication services. The misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

RESPONSIBILITIES AND OBLIGATIONS

Supporting students to use digital devices and online services in safe, responsible and respectful ways is a shared responsibility.

For students

- Be safe, responsible and respectful users of digital devices and online services, and support their peers to be the same.
- Respect and follow school rules and procedures and the decisions made by staff, knowing that other schools may have different arrangements.
- Communicate respectfully and collaboratively with peers, school staff and the school community and behave in the ways described in the Behaviour Code for Students. See Below.

For parents and carers

- Recognise the role they play in educating their children and modelling the behaviours that underpin the safe, responsible and respectful use of digital devices and online services.

- Support implementation of the school procedure, including its approach to resolving issues.
- Take responsibility for their child's use of digital devices and online services at home such as use of online services with age and content restrictions.
- Communicate with school staff and the school community respectfully and collaboratively as outlined in the [School Community Charter](#).
- Switch off or put their digital devices on silent when at official school functions, during meetings and when assisting in the classroom.
- Provide digital devices that meet school specifications where a school is participating in a bring your own device program and complete any related paperwork.

For the principal and teachers

- Deliver learning experiences that encourage safe, responsible and respectful use of digital devices and online services. This includes:
 - Establishing agreed classroom expectations for using digital devices and online services, in line with this procedure and departmental policy.
 - Identifying strategies to ensure that all students are able to engage in classroom activities including strategies to accommodate students without a digital device.
 - Reading and abiding by the Terms of Service for any online services they use in teaching, including those limiting use by age.
 - Educating students about online privacy, intellectual property, copyright, digital literacy and other online safety related issues.
- Model appropriate use of digital devices and online services in line with departmental policy.
- Respond to and report any breaches and incidents of inappropriate use of digital devices and online services as required by school procedures, departmental policy and any statutory and regulatory requirements. This includes:
 - Reporting the creation, possession or distribution of indecent or offensive material to the Incident Support and Report hotline as required by the Incident Notification and Response Policy and Procedures and consider any mandatory reporting requirements.
 - Working with the department and the Office of the eSafety Commissioner (if necessary) to resolve cases of serious online bullying and image-based abuse.
 - Following the school's behaviour management plan when responding to any incident of inappropriate student behaviour relating to the use of digital devices or online services.
- If feasible and particularly as issues emerge, support parents and carers to understand strategies that promote their children's safe, responsible and respectful use of digital devices and online services.
- Participate in professional development related to appropriate use of digital devices and online services.

For non-teaching staff, volunteers and contractors

- Be aware of the department's policy, this procedure and act in line with the conduct described.
- Report any inappropriate use of digital devices and online services to the principal, school executive or school staff.

COMPLAINTS

If a student, parent or carer has a complaint under this procedure, they should first follow our school's complaint process. If the issue cannot be resolved, please refer to the department's [guide for students/parents/carers about making a complaint about our schools](#).

EXEMPTIONS

Exemptions to any part of this procedure may apply for some students in some circumstances. Parents and carers can request an exemption and these will be considered on a case-by-case basis and granted when required by law or at the principal's discretion.

REVIEW

The principal or delegated staff will review this procedure annually.

KEY TERMS

Digital citizenship refers to the skills and knowledge a person needs to effectively use digital technologies in a positive way so they can participate in society, communicate with others, and create and consume digital content.

Digital devices are electronic devices that can receive, store, process and share digital information and connect to applications (apps), websites and other online services. They include desktop computers, laptops, tablets, smartwatches, smartphones and other devices.

Digital literacy is the set of social, emotional and technological skills and competencies that people need to understand to use digital devices and online services, and to expand their opportunities for education, employment and social participation, including entertainment.

Educational purpose is any use approved by school staff that supports student learning, wellbeing and educational outcomes.

General capabilities are the broad collection of knowledge, skills, behaviours and dispositions described within the Australian curriculum and NSW syllabus.

Image-based abuse occurs when intimate, nude or sexual images are distributed, or threatened to be distributed, without the consent of those pictured. This includes real, altered and drawn pictures and videos. This is a crime in NSW.

Online bullying involves *using technology such as the internet or mobile devices to bully someone. Bullying behaviour has three key features. It involves the intentional misuse of power in a relationship. It is ongoing and repeated, and it involves behaviours that can cause harm. Bullying behaviour can also involve intimidation, victimisation and harassment, including that based on sex, race, religion, disability, or sexual orientation.*

Online safety is the safe, responsible and respectful use of digital media, devices, other technology and online services.

Online services are any software, website or application that can gather, process or communicate information. This includes digital classrooms, chat and messaging, online games, virtual reality, social media and other online spaces.

Reasonable adjustment is a measure or action taken to assist a student with disability to participate in education and training on the same basis as other students.

School-related settings include school grounds, school-related activities and outside of school where there is a clear and close connection between the school and the conduct of students. This connection may exist in situations where: there is discussion about school taking place outside of school hours; a student is wearing their school uniform but is not on school premises; a relationship between parties commenced at school; students are online in digital classrooms; and where online contact has flow on consequences at school and duty of care requires the school to respond once an incident is reported.

School staff refers to school personnel who have some level of responsibility for implementing policy and the school digital devices and online service procedure. This includes principals, senior staff, teachers, non-teaching staff, school administrative staff, volunteers and contracted staff engaged by schools.

Sailing the Sea of Excellence

BEHAVIOUR CODE

What is safe, responsible and respectful student behaviour?

Be SAFE

- Protect your personal information, including your name, address, school, email address, telephone number, pictures of you and other personal details.
- Only use your own usernames and passwords, and never share them with others.
- Ask a teacher or other responsible adult for help if anyone online asks for your personal information, wants to meet you or offers you money or gifts.
- Let a teacher or other responsible adult know immediately if you find anything online that is suspicious, harmful, inappropriate or makes you uncomfortable.
- Never hack, disable or bypass any hardware or software security, including any virus protection, spam and filter settings.

Be RESPONSIBLE

- Follow all school rules and instructions from school staff, including when using digital devices and online services.
- Take care with the digital devices you use.
 - Make sure the devices you bring to school are fully charged each day and are stored appropriately when not in use.
 - Understand that you and your parents and carers are responsible for any repairs or IT support your personal devices might need.
 - Make sure the devices you bring to school have the latest software installed.
 - Take care with the school-owned devices you share with others, so that other people can use them after you.
- Use online services in responsible and age-appropriate ways.
 - Only use online services in the ways agreed to with your teacher.
 - Only access appropriate content and websites, including when using the school's filtered network and personal, unfiltered networks.
 - Do not use online services to buy or sell things online, to gamble or to do anything that breaks the law.
- Understand that everything done on the school's network is monitored and can be used in investigations, court proceedings or for other legal reasons.

Be RESPECTFUL

- Respect and protect the privacy, safety and wellbeing of others.
- Do not share anyone else's personal information.
- Get permission before you take a photo or video of someone, including from the person and from a teacher.
- Do not harass or bully other students, school staff or anyone, this includes cyber bullying using a digital device or online service.
- Do not send or share messages or content that could cause harm, including things that might be:
 - inappropriate, offensive or abusive;
 - upsetting or embarrassing to another person or group;
 - considered bullying;
 - private or confidential; and/or
 - a virus or other harmful software.

Sailing the Sea of Excellence