DIGITAL LEARNING POLICY

Contents

Digital Learners at Seaview High School

Seaview High School is an innovative, inclusive and safe school that delivers relevant curriculum and promotes rigour, relationships and lifelong learning.

Rationale

The Digital Learning program for all students facilitates enhanced pedagogies to engage all students with the curriculum. The program provides a vehicle for personalised learning and supports a constructivist approach to curriculum development and delivery.

In keeping with the National Educational Goals for Young Australians, we aim to promote and lead world's best practice for curriculum delivery and assessment and improve educational outcomes for all students.

This policy provides direction to staff, students and parents/caregivers on procedures, responsibilities and expectations with regard to Digital Learning at Seaview.

Student Devices

Current research suggests that the interactivity provided by tablets is ideally suited to Middle School student learning. The Digital Learning Program at Seaview includes the use of iPads at Years 8 and 9, and a range of preferred laptops for students in Years 10 to 12. The program is a Bring Your Own Device (BYOD) program, which means the iPad and laptop are purchased by the parent/caregiver and belong to the student. After extensive community consultation the school has identified a number of recommended devices that we believe will best support quality teaching and learning. We are pleased to be able to offer our families an online portal for purchasing all of the recommended devices, at highly competitive prices.

Policy Development

Extensive research and consultation with all stakeholders will be ongoing to ensure our Digital Learning program and policies remain aligned to the school's strategic plan.

Loss, theft or accidental damage to student owned devices

All devices purchased by families belong to the student. The school will not take responsibility for any loss, theft or damage that occurs to student owned devices.

Insurance

Seaview strongly recommends families add student owned devices to their 'Home and Contents' Insurance. Families are encouraged to insure the devices at home, at school and in transit to and from school.

Social Justice/Financial Hardship
Families experiencing financial hardship may apply to the school for assistance with funding for Digital Learning resources. Applications will be assessed on an individual basis by the Business Manager)

Ownership
Student owned devices remain the property of the student; however, whilst connected to the Seaview High School network, students must adhere to the school's iPad and/or Laptop User agreement.

General Policy

(Including expectations of students and the responsibilities of staff and parents/caregivers)

Acceptable Use

1. Students are expected to take their device to all lessons unless the teacher has requested otherwise. Teaching and learning programs will make use of digital technology to enhance learning through inquiry, collaboration and new ways of demonstrating knowledge.

2. Any illicit material, including photos, movies/TV series/game downloads etc. found on a student device will result in suspension and/or exclusion from school. Where a student is suspected of any unlawful activity, the device will be confiscated and the matter referred to SAPOL.

3. The use of student owned devices is on the understanding that students will follow teacher instructions and access applications and files in safe and ethical ways. Students must not disrupt the smooth running of any school ICT systems nor attempt to hack or gain unauthorised access to any system.

4. The LearnLink Office 365 Service, including Office 365 Pro Plus is only to be used in relation to delivering curriculum objectives, and must not be used to store sensitive or personal information.

5. Seaview High School reserves the right to monitor the content of student owned devices and may conduct live monitoring of activity whilst a student is at school. Students must permit school staff and parents/caregivers to perform checks when requested. Parents/caregivers will be informed of any inappropriate use.

6. Consequences for inappropriate use will be in accordance with Seaview High School's Behaviour Management Policy and may include disconnection of a student device from the school network for a period of time or managed privileges, at the discretion of school leadership. Teachers may also elect to confiscate a student device until the end of a lesson where it is not being used appropriately.

7. The camera application is only to be used in class with teacher permission. Photos of another person must be with their permission only.

8. The Casper (JAMF) Management software (or other MDM utilized by the school), and its associated profiles/files, must remain installed and operational on the student iPads at all times.

Cyber Safety

Staff, students and parents/caregivers should familiarise themselves with the following document:
https://www.decd.sa.gov.au/sites/g/files/net691/f/cyber-bullying-e-crime-and-the-protection-of-children-and-young-people-advice-for-families.pdf).

"Learning is a social activity. It happens when people interact with other people and their ideas, knowledge and perspectives. ICTs provide children and students with new and engaging ways to learn. ICTs expand social and knowledge networks so that children and students access current information, interact with experts and participate in peer teaching and learning.

Using ICTs they can publish their learning, as evidence of achievement or to invite feedback for improvement. It is important to both protect and teach children, students and adults, while they learn to use ICTs and become responsible digital citizens. This includes adults thinking ahead of new risks and children and students learn how to avoid exposure to inappropriate material or activities, and protecting themselves when they are online. They need to learn how to use ICTs, including mobile technologies and social networking sites, in responsible and ethical ways. In addition, they need to feel confident about alerting the adults in their lives when they are feeling unsafe, threatened, bullied or exposed to inappropriate events. In response, these adults need to take appropriate actions to protect the child or young person."

Key aspects of Cyber Safety include:

- Students must not give out identifying information online, use only their first name and not share their home address, telephone number or any other personal information such as financial details (e.g. credit card), telephone numbers or images (video or photographic) of themselves or others.
- Students must not use their school e-mail address in non-school online communications as this e-mail address contains their personal name and school details.
- Students must use the Internet, e-mail, mobile phones or any ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.
- Students must not forward inappropriate material to others.
- Students should never respond to message or bulletin board items that are suggestive, obscene, belligerent, threatening or make them feel uncomfortable - these messages should be reported to a teacher.
- Students must inform their teacher immediately if they see anything on a website that is inappropriate, unpleasant or makes them uncomfortable.
- Parents/caregivers and teachers should actively monitor online behaviour and encourage their child/student to follow Cyber-safe strategies.

Internet Usage at School
According to DECD ICT Security, Internet Access and Use, and Electronic Mail and Use policies, students may use the Internet only for learning related activities that are approved by a teacher. They must not cause interference or disruption to other people or equipment, and students may not access or distribute inappropriate material. This includes:

- distributing spam messages or chain letters
- accessing or distributing malicious, offensive or harassing material, including jokes and images
- bullying, harassing, defaming or giving offence to other people
- spreading any form of malicious software (e.g. viruses, worms)
- accessing files, information systems, communications, devices or resources without permission
- using for personal financial gain
- using non-approved file sharing technologies (e.g. Torrent)
- using for non-educational related streaming audio or video
- using for religious or political lobbying
- downloading or sharing non-educational material.

While Seaview High School will make every reasonable effort to provide a safe and secure online learning experience for children and students, Internet filtering is not 100 per cent effective and it is not possible to guarantee that children and students will not be exposed to inappropriate material.

The cost to access the Internet at school is currently included in the school fee and allows for students to make reasonable use of the Internet for the purpose of learning. Internet traffic is monitored and students making unreasonable downloads may have network access limited.

Internet Usage at Home
Internet browsing by students at home or from other non-DECD sites is permitted. **Please note this will not be filtered or monitored by Seaview High School.**

Students using their own device at home to access the Internet should do so in a safe and ethical manner. Parents/caregivers should actively monitor and discuss their child's safe use of the Internet.

Passwords
DECD ICT Security and Internet Access and Use policies contain the following main provisions with regard to passwords:

- Passwords must be kept confidential and not displayed or written down in any form.
- Passwords must not be words found in a dictionary, or based on anything somebody else could easily guess or obtain using person-related information.
- Students must not disclose their personal passwords to any person other than Seaview IT staff and Principal Team members, or where Seaview High School IT Support is required.

- Students will be accountable for any inappropriate actions (eg bullying, accessing or sending inappropriate material) undertaken by someone using their personal network logins.

Copyright
Students must realise their responsibilities regarding intellectual property and copyright law and ethics, including acknowledging the author or source of information. To ensure compliance with copyright laws, students must only download or copy files such as music, videos or programs, with the permission of the owner of the original material. If students infringe the Copyright Act 1968, they may be personally liable under this law.

Printing
Seaview High School is committed to improving the environment. Staff and students are encouraged to transmit work electronically and lessen the need to print documents. Students will be permitted to print to printers from all devices. Printing restrictions and charges apply.

Software installation, games and music
Students and parents will have Administrator access to their device, and are permitted to install software and files provided they have acquired a legitimate license. Student installed software must be educational in nature or have a direct relationship to student learning. Non-educational software, games and music are not recommended as they will use space unnecessarily on the hard drive and therefore impede use of the device for learning. In instances where device performance is identified as lagging due to student installed software and files, a recommendation to parents regarding removal of software will be made.
Under no circumstances should software and files be installed without the appropriate license. Students doing so may be liable to prosecution. Parents/caregivers are encouraged to monitor the contents of the device regularly.

Social Networking
Under certain circumstances social networking sites may be beneficial for learning. However, in many instances social networking sites can be a distraction and potentially unsafe. Students must seek permission from their teacher or parent/caregiver before accessing social networking sites at school.

Students using social networking sites without permission during lessons will be subject to consequences according to the 'Acceptable Use' section.

Students are reminded to use Cyber-safe strategies and use the Internet in a safe and ethical manner.

Mobile Device Management
A Mobile Device Management (MDM) system will be installed on all iPads in order to improve productivity in class, help prevent distraction, assist in locating lost or stolen devices, and allow the school to provide additional software free of charge. Seaview uses the Casper (JAMF) system for MDM.

The MDM system is mandatory and must be installed on your iPad. Should it be detected that the MDM has been removed; the student will lose access to all school systems on their devices until it is re-instated.

Seaview High School cannot see any personal information, email, photos, messages, Apple Accounts, access the camera or obtain credit card details on devices connected through the MDM system. Only the owner of an Apple ID can authorise purchases, and no location tracking data is stored by Seaview High School.

Training and Development
Training and development will be provided at the start of Year 8 to students in order to familiarise them with the iPad. Further help can be obtained from the IT Support desk as required.

Health, Safety and Welfare
Students are advised to consider the following advice when using their personal devices:

- taking regular rest breaks within the confines of the classroom and at the discretion of the teacher
- not using the device for more than 2 hours in any one session
- working in an environment free from glare
- using their laptop on a desk rather than on their lap whenever possible
- angle the screen to minimise the need to bend the neck
- maintaining good posture.

The main feature of mobile devices that causes problems is the minimal amount of ergonomic
adjustment – this promotes poor posture. Students should be aware of their mobility while using their device.

Preventing Eye Strain
Eye-strain and headaches can be caused by the constant viewing of small objects on small screens, incorrect monitor position, or glare or reflection from lighting sources. The risk of eye-strain can be reduced by ensuring students:

- work in environments free from glare or reflection
- have adequate lighting
- increase font size for comfortable viewing
- position the screen for comfortable viewing distance
- take frequent breaks from the screen, for example: every 20 minutes look at something 20 feet away (approx 6 metres) for 20 seconds
- regularly blink to lubricate your eyes.