

DIGITAL LEARNING POLICY

Digital Learning Program Policy 2021

Table of Contents

Digital Learning Program Policy 2021	2
Learners at Brighton Secondary School	3
Rationale	3
Devices at Brighton	3
Policy Development	3
Loss, theft or accidental damage to the iPad	3
Insuring the iPad	3
Loss, theft or accidental damage to the MacBook	3
Travelling with the MacBook	4
Insuring the Macbook	4
Loan MacBooks	4
Ownership of the Macbook	4
MacBook Payments	4
General Policy	5
Acceptable Use	5
Cyber Safety	6
Internet Usage at School	6
Internet Usage at Home	7
Passwords	7
Copyright	7
Printing	7
Software installation, games and music	7
Social Networking	8
Parental Control	8
Private Laptops and Personal Devices	8
Mobile Device Management	8
Cloud Services	
Training and Development	9
Occupational Health Safety and Welfare	9

Learners at Brighton Secondary School

Brighton Secondary School is an innovative, safe school that delivers relevant curriculum and promotes rigour, relationships and lifelong learning.

Rationale

The Digital Learning program for all students enables change in pedagogical practices to engage students with the curriculum. The program provides a vehicle for a personalised learning program and supports a constructivist approach to creating curriculum.

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

This policy provides direction to staff, students and parents/caregivers on procedures, responsibilities and expectations with regard to the Digital Learning program. The Governing Council has endorsed the program and approved the financial commitment based on a formal poll of parents/caregivers.

Devices at Brighton

Current research suggests that the interactivity of tablets is very suited to Middle School students. Consequently, the Digital Learning Program was modified in 2014 to include iPads (Years 8 and 9) and MacBooks (Years 10 to 12). This was endorsed via a formal poll of parents/caregivers.

The iPad program is a Bring Your Own Device (BYOD) program, which means the iPad is purchased by the parent/caregiver and belongs to the student from the outset.

The MacBook program is a School-Owned Device program, which means that the Macbook is initially purchased and owned by the school, with the parent/caregiver paying for the device over three years, and ownership transferring at the conclusion of the student's schooling.

Policy Development

Extensive research and consultation with all stakeholders will continue to occur in order to review the Digital Learning program and policies to ensure alignment with the school's strategic plan.

Loss, theft or accidental damage to the iPad

As the iPad belongs to the student, the school will not take responsibility for any loss, theft or damage.

Insuring the iPad

Brighton Secondary School strongly recommends families add the iPad as an item on their own 'Home and Contents' Insurance.

Ownership of the iPad

The iPad belongs to the student or parent/caregiver. However, the student is required to abide by the *iPad Use Agreement* signed by the student and his or her parent/caregiver at the start of the school year.

Loss, theft or accidental damage to the MacBook

Where a loss, theft or damage is the result of malice, carelessness, inattention or apparent disregard for the laptop, parents/caregivers will be charged for the repair or replacement cost of a new MacBook.

Brighton Secondary School will only replace or repair student MacBooks under the following conditions:

- Carelessness, inattention, apparent disregard, or malice are ruled out
- The student submits a MacBook Support Request form, available from the IT Services Office or Student Reception
- Stolen/Lost laptops must be reported immediately by the student or parent/caregiver to the police and provide the school with the police report number on the *MacBook Support Request* form.

In the case of theft, loss or accidental damage to the MacBook, repairs or replacement will occur at the discretion of the school.

The *MacBook Support Request* form are available from the IT Services Office or Student Reception. Parents/caregivers may obtain the form from the Front Office. Completed forms should be submitted to the IT Services Office where they will be considered by the IT Systems Leader. The IT Systems Leader will decide on the recommendation based on available evidence.

Travelling with the MacBook

As all MacBooks remain the property of the South Australian Minister for Education for the duration of the program, MacBooks are not to be taken away on holiday for any reason, unless formally requested by a staff member for excursions. This includes interstate and overseas travel.

Insuring the Macbook

Brighton Secondary School strongly recommends families add the supplied MacBook as an item on their own 'Home and Contents' Insurance.

Loan MacBooks

Loan MacBooks may be available from the IT Services Office.

If a student must await the repair or replacement of their MacBook they may receive approval to borrow a MacBook for the duration of the repair/replacement period, which will not exceed one school term. The MacBook must be returned to the IT Services Office for re-imaging at the end of the loan period.

Any 'loan' MacBook still in student possession at the end of term must be returned to the IT Services Office before the start of the school holidays. Failure to do so will result in school consequences and the privilege of using a 'loan' MacBook revoked in the future. If the loan is not returned before leaving Brighton Secondary School, parents/caregivers may be billed for the cost of a new replacement.

Ownership of the Macbook

All MacBooks remain the property of the South Australian Minister for Education for the duration of the program. Brighton Secondary School will dispose of the MacBook at the end of life, i.e. three years, by transfer of ownership to student.

This will only occur if the student completes Year 12. At this time, students will be required to return the MacBook to the school's IT Services to remove school licensed software and process the MacBook for transfer of ownership. Any student who fails to have school licensed software removed may be liable to copyright infringement as per the Copyright Act 1968.

If a student leaves the school prior to the completion of the program (i.e. before the end of Year 12) they must return the MacBook to the school's IT Services and pay for any damage to the MacBook. Alternately, the parent/caregiver may opt to 'buyout' the device in which case, contact Student Reception.

Students who enrol at the school in Year 10, 11 or 12 will be provided with a laptop under similar conditions.

MacBook Payments

Parents/caregivers of students in Years 10, 11 and 12 will be invoiced yearly for one-third of the cost of the device, for a total of three years. A 'Commitment to Pay' form must be signed prior to receiving the device. Any default on payments will be legally recovered.

General Policy

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

Acceptable Use

- 1. Students must take the device to all lessons unless the teacher has requested otherwise. Teaching and learning programs will make use of the device to benefit students' learning through inquiry, collaboration and new ways of demonstrating knowledge.
- 2. Off-task behaviour will be subject to consequences in line with Brighton Secondary School's Behaviour for Learning policy.
- 3. Any illegal or offensive material found on a device will result in suspension and/or exclusion from school. Illegal or offensive material includes, but is not limited to, pornographic material, illegally downloaded games/movies/TV series etc. The South Australian Police will be notified regarding any unlawful activity.
- 4. The use of the device 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. The school's wellbeing and Behaviour for Learning processes, and this Digital Learning policy, extend outside of school hours and off-site.
- 5. Brighton Secondary School reserves the right to monitor the content of student device and may conduct live monitoring of activity on the device while the device is at school. Students must permit school staff and parents/caregivers to perform checks when requested and may have 'Parental Control' enabled by the school at the school's discretion.
- 6. Teachers and parents/caregivers may recommend a particular student's device has 'Parental Control' features activated, which limit the student's privileges and means they will be unable to install software. These limited privileges may include restricting access to particular websites, times of day, software, mail and/or messaging applications.
- 7. Consequences for inappropriate use will be in accordance with Brighton Secondary School's Behaviour for Learning policy and may include confiscation of the device for a period of time or managed privileges, at the discretion of Faculty Leaders, Year Level Managers or other School Leadership staff who will store the device and be responsible for all communication with regard to return of the device. Where a student is suspected of any unlawful activity, it will be reported to the South Australia Police.
- 8. At the discretion of the school, a student's device screen may be displayed at any time to staff, students or visitors to the school. Students' screens may be shared on any of the large display screens in the school.
- 9. When a pattern of non-attendance is identified, student MacBooks may be confiscated until attendance improves.
- 10. When a student is suspended, their MacBook may be confiscated for the period of the suspension.
- 11. The AirDrop function on the device is to be switched off at school at all times, unless required by a member of staff.

- 12. The device's name must be set to 'firstname.lastname', and must not be changed. (For example, Ada Lovelace's device would be named 'ada.lovelace'.)
- 13. The camera is only to be used in class with teacher permission. Photos of another person must be with their permission.
- 14. The JAMF Mobile Device Management software (or other MDM utilized by the school), and its associated profiles/files, must remain installed and operational on the device at all times.
- 15. The Apple Classroom feature of the device must be installed and operational at all times.

Cyber Safety

Staff, students and parents/caregivers must familiarise themselves with the content of the eSafety Comissioner's Online Safety Book, available at https://www.esafety.gov.au/parents/online-safety-book

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 messages 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 the Department for Education 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
- using for non-educational related streaming audio or video
- using for religious or political lobbying
- · downloading or sharing non-educational material.

While Brighton Secondary 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 incur an additional fee.

Internet Usage at Home

Internet browsing by students while they are off-site, for example at home, is permitted. Please note this will not be filtered or monitored by Brighton Secondary School.

Brighton Secondary School accepts no cost for home internet provision. In order to ensure equity of access to the curriculum, students will have at least two nights to complete school learning tasks that require compulsory internet access outside of the subject lesson.

Your Internet Service Provider provides home internet logon details, and it is the responsibility of the student/parent/caregiver to setup the Home-Internet connection on the device (generic instructions will be provided.)

Students using their device at home to access the internet must do so in a safe and ethical manner, with parental permission – please refer to the 'Parental Control' section for details of how parents can use the operating system to monitor student internet activity. Parents/caregivers should actively monitor and discuss their child's use of the internet.

Passwords

Department for Education 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 BSS IT staff and Principal Team members, and except on Brighton Secondary School IT Support request forms.
- Students will be accountable for any inappropriate actions (eg bullying, accessing or sending inappropriate material) undertaken by someone using their personal log-on details.

Copyright

Students must be aware of 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

Staff and students are encouraged to transmit work electronically and lessen the need to print documents. Students will be permitted to print from all devices. Printing restrictions and charges apply.

Software installation, games and music

Students may have Administrator access to their device and may be permitted to install certain types of 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 unnecessarily use space on the device and therefore impede its use for learning. Students using non-educational software, games and files at school will be subject to consequences according to the 'Acceptable Use' section. In instances where the device's performance is restricted due to student installed software and files the device's storage may be erased and re-imaged by IT Services.

Under no circumstances may software and files be installed without the appropriate license. Students doing so will be liable to prosecution.

Parents/caregivers are encouraged to regularly monitor the contents of the device.

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.

School Internet filters block many social networking sites. Parents wishing to filter home internet on the device should refer to the section titled 'Parental Control'.

Students using social networking sites without permission during lessons will be subject to consequences according to the school's Behaviour for Learning policy.

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

Parental Control

The devices are preloaded with 'Parental Control' capabilities. By default, these are turned off. Parents/caregivers seeking to manage, monitor, and control the time their child spends on the device, including the sites they visit, can request that Parental Control be turned on.

In the event that a parent/caregiver would like to turn on 'Parental Control' they must complete and return a Support Request form to the IT Services Office. These forms are available from the IT Services Office, Student Reception and the Front Office.

Please note that the implications of turning on 'Parental Control' include:

- The school or parent/caregiver will have an administrator account on the device.
- The student will no longer have administrative privileges to the device.
- The student will no longer be able to change settings or install software unless the parent/caregiver is present to enter their password the school will not provide ICT Support in this instance.

Private Laptops and Personal Devices

Private laptops and personal devices add complexity to the functionality and maintenance of the school network. Only BYOD iPads and school-owned MacBooks, providing they have the standard image applied, can be supported by the school.

Only staff, students, and other school-approved users are permitted to access the school's network.

Mobile Device Management

A Mobile Device Management (MDM) system will be installed on all devices 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.

The MDM system is mandatory and must be installed on the device. 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.

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

Apple's Classroom functionality may be used on all devices in order to share resources, improve productivity in class and help prevent distraction. Teachers will be able to see what students are working on while in their class, however they cannot see students' sensitive information or access this off-site.

Cloud Services

Office 365 is a service provided for students and supported by the Department for Education for use in schools. This allows Office products to be downloaded onto devices. It also enables collaboration among students on documents, and ongoing backup of student work.

Training and Development

Training and development will be provided in order to familiarise students and their parents or caregivers with the device. It is expected that parents/caregivers and students will attend an initial session in order to receive their device. Additional videos and/or sessions will cover:

- Welcome to your device
- Cyber Safety
- · Using the device for learning

Occupational Health Safety and Welfare

Students are advised to consider the following advice when using their device:

- · 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 the device on a desk rather than on the lap whenever possible
- angle the screen to minimise the need to bend the neck
- maintaining good posture.

CYBER-SAFETY AT BRIGHTON SECONDARY SCHOOL

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Brighton Secondary School are based on our core values. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this document and sign the attached Use Agreement Form.

Rigorous cyber-safety practices are in place, which include Use Agreements for staff and students, who have been involved in the development of the agreement. 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.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at Brighton Secondary School, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school, and used on or off the site.

The overall goal of Brighton Secondary School is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The Use Agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

All students will be issued with a Use Agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment.

Material sent and received using the network may be monitored, and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail. Where a student is suspected of an electronic crime, this will be reported to the South Australia Police. Where a personal electronic device such as a mobile phone is used to capture images of a crime, such as an assault, the device will be confiscated and handed to the police.

While every reasonable effort is made by schools and DfE administrators to prevent student's exposure to inappropriate content when using the department's online services, it is not possible to completely eliminate the risk of such exposure. In particular, DfE cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DfE recommends the use of appropriate Internet filtering software.

More information about Internet filtering can be found on the websites of the Australian Communications and Media Authority at http://www.acma.gov.au, NetAlert at http://www.netalert.gov.au, the Kids Helpline at http://www.kidshelp.com.au and Bullying No Way at http://www.bullyingnoway.com.au.

Please contact the principal, if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.

Important terms:

'Cyber-safety' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

'Cyber bullying' is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, social media platforms, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person.

'School and preschool ICT' refers to the school's or preschool's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.

'ICT equipment/devices' includes computers (such as desktops and laptops), storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies.

'Inappropriate material' means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school or preschool environment.

'E-crime' occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

Strategies to help keep Brighton Secondary School Students Cyber-safe

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices for themselves and the people around them regardless of the time of day. Being cyber-safe is no exception and we invite you to discuss with your child the following strategies to help us stay safe when using ICT at school and after formal school hours.

- 1. I will not use school ICT equipment until my parents/caregivers and I have signed my Use Agreement Form and the completed form has been returned to school.
- 2. If I have my own user name, I will log on only with that user name. I will not allow anyone else to use my name.
- 3. I will keep my password private.
- 4. While at school or a school related activity, I will inform the teacher of any involvement with any ICT material or activity that might put me or anyone else at risk (eg bullying or harassing).
- 5. I will 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.
- 6. I will use my mobile phone/s only at the times agreed to by the school during the school day.
- 7. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.
- 8. While at school, I will:
 - access, attempt to access, download, save and distribute only age appropriate and relevant material
 - report any attempt to get around or bypass security, monitoring and filtering that is in place at school.
- 9. If I accidentally access inappropriate material, I will:
 - not show others
 - turn off the screen or minimise the window
 - report the incident to a teacher immediately.
- 10. To ensure my compliance with copyright laws, I will download or copy files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material. If I infringe the Copyright Act 1968, I may be personally liable under this law. This includes downloading such files as music, videos, games and programs.
- 11. My privately owned ICT equipment/devices, such as a laptop, mobile phone, USB/portable drive I bring to school or a school related activity, also is covered by the Use Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.
- 12. Only with written permission from the teacher will I connect any ICT device to school ICT, or run any software (eg a USB/portable drive, camera or phone). This includes all wireless/Bluetooth technologies.
- 13. I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following:
 - my full name
 - my address
 - my e-mail address
 - my phone numbers
 - photos of me and/or people close to me.
- 14. I will respect all school ICTs and will treat all ICT equipment/devices with care. This includes:
 - not intentionally disrupting the smooth running of any school ICT systems
 - not attempting to hack or gain unauthorised access to any system.
 - following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICTs
 - reporting any breakages/damage to a staff member.

- 15. The school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including e-mail.
- 16. The school may monitor and audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including e-mail.
- 17. If I do not follow cyber-safe practices, the school may inform my parents/caregivers. In serious cases, the school may take disciplinary action against me. My 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.

DIGITAL LEARNING POLICY USE AGREEMENT



Before being granted access to Brighton Secondary School's Information & Communication Technology (ICT) systems, and/or being issued with a Brighton Secondary School laptop, students and parent(s) must read the Digital Learning Policy which includes the Cyber-Safety, understand its contents, and sign and return this Acceptable Use Agreement to the school.

You should keep the Digital Learning Policy for which this agreement applies for future reference.

STUDENT AGREEMENT

My responsibilities include:

- · Reading this Use Agreement carefully
- following the school's Digital Learning policy whenever I use the school's ICTs
- following the cyber-safety strategies whenever I use privately-owned ICT devices on the school site or at any school related activity, regardless of its location
- avoiding any involvement with material or activities that could put at risk my own safety, or the privacy, safety or security of the school or other members of the school community
- taking proper care of school ICTs. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, I and/or my family may have responsibility for the cost of repairs or replacement
- Keeping this document somewhere safe so I can refer to it in the future
- asking the Digital Pedagpgy Leader if I am not sure about anything to do with this agreement.

PARENT/LEGAL GUARDIAN AGREEMENT

My responsibilities include:

- I have read and understood this Digital Learning Policy Use Agreement carefully and discussing it with my child so we both have a clear understanding of our roles in the school's work to maintain a cyber-safe environment
- ensuring this Use Agreement is signed by my child and by me and returned to the school
- encouraging my child to follow the cyber-safe strategies and instructions
- contacting the school if there is any aspect of this Use Agreement I would like to discuss
- I am aware that signing and returning this form constitutes a commitment by me, the parent/caregiver/legal guardian, to pay such costs, and that Brighton Secondary School's policies relating to the recovery of debts will apply.

Please note: This agreement will remain in force as long as your child is enrolled at this school. If it becomes necessary to add/amend any information or rule, you will be advised in writing.

For further information regarding the device program, please email IT Systems Leader dl.0803.ictsupport@schools.sa.edu.au

For assistance with financial aspects of the program please email Finance dl.0803.finance@schools.sa.edu.au

We have read and understood this Digital Learning Policy Use Agreement and we are aware of the school's initiatives to maintain a cyber-safe learning environment.

Name of student	Group /Class
Signature	Date
Name of parent/caregiver/legal guardian	
Signature	Date