# BRIGHTON BEACH PRIMARY SCHOOL

# DIGITAL LEARNING
## (INTERNET, SOCIAL MEDIA and DIGITAL DEVICES)

**Help for non-English speakers**

If you need help to understand this policy, please contact Brighton Beach Primary School brighton.beach@education.vic.edu.au or 9591 0888

## PURPOSE

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 including our iDay and 1:1 Bring Your Own Device (BYOD) program.
(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
(e) the various Department policies on digital learning, including social media, that our school follows and implements when using digital technology
(f) our school prioritises the safety of students whilst they are using digital technologies
(g) educating students about safe and responsible behaviour online is best taught in partnership between home and school

## SCOPE

This policy applies to all students and staff at Brighton Beach Primary School.

Staff use of technology is also governed by the following Department policies:

- Acceptable Use Policy for ICT Resources
- Cybersafety and Responsible Use of Digital Technologies
- Digital Learning in Schools and
- Social Media Use to Support Student Learning.

Staff, volunteers and school councillors also need to adhere to codes of conduct relevant to their respective roles. These codes include:

- BBPS Child Safety Code of Conduct
- The Victorian Teaching Profession Code of Conduct (teaching staff)
- Code of Conduct for Victorian Sector Employees (staff)
- Code of Conduct for Directors of Victorian Public Entities (school councillors)

## DEFINITIONS

For the purpose of this policy, "digital technologies" are defined as digital devices, tools, applications and systems that students and teachers use for learning and teaching; this includes Department-provided software and locally sourced devices, tools and systems.

## POLICY

### Vision for digital learning at our school

The use of digital technologies is a mandated component of the Victorian Curriculum F-10.

Safe and appropriate use of digital technologies, including the internet, apps, computers and tablets, can 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 learning that is interactive, collaborative, personalised, engaging and transformative. 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.

Brighton Beach 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 safely and appropriately to reach their personal best and fully equip them to contribute positively to society as happy, healthy young adults.

### Personal Devices at Brighton Beach Primary School

Brighton Beach Primary School operates a Bring Your Own Device (BYOD) iPad program.

Parents/carers are invited to purchase an iPad for their child to bring to school. Brighton Beach Primary School provide parents/carers with the opportunity to purchase an iPad through JB Education at a discounted price. Through the JB Education portal, parents also have the opportunity to purchase iPad accessories, insurance and AppleCare. If students are unable to purchase their own iPad, Brighton Beach Primary School will provide them with a device to use during school hours. The school can refer parents to government or community support programs that may help them if they wish to purchase a device for their child to own, rather than use what is provided for free by the school.

Students are invited to bring their own device to school each day to be used during class time for different learning activities. When bringing their own device to school, students should ensure that it:

- Is fully charged each morning
- Is brought to school in a protective case
- Is regularly updated so it is running on the latest possible OS version

Please note that our school does not have insurance to cover accidental damage to students' devices, and parents/carers are encouraged to consider obtaining their own insurance for their child's device.

Students, parents and carers who would like more information or assistance regarding our BYOD program are encouraged to contact the classroom teacher.

Further information is provided through the following documents:

- BBPS Acceptable Use Agreement for Internet and Digital Technologies 3 – 6
- BBPS Acceptable Use Agreement for Internet and Digital Technologies Prep – 2
- Grade 3 iDay Acceptable Use Agreement
- 1:1 iPad Acceptable Use Agreement

**Responsibilities**

Staff responsibilities:

All staff members are to be familiar with this policy and information contained in the documents listed above. Staff are to familiarise themselves at the beginning of each school year with each policy document and carry out the necessary requirements within their classroom and as part of their daily duties while at school

At the beginning of each school year, and at any other time as needed, teachers are to familiarise the students with the protocols in place for using digital technologies, including both the safe handling of equipment together with the penalties imposed if incorrect use occurs

Student responsibilities:

- Throughout each school year, students will receive explicit education in relation to:
- Staying safe online
- How to deal with conflict, bullying, cyber-bullying and harassment
- Building confidence, resilience, persistence, relationships and organisational skills.

Staff will use the following resources to enhance their teaching of an digital technologies curriculum:

- eSafety – Office of the Children's eSafety Commissioner
- eSmart School Program
- Incursions and Excursions, such as Project Rockit

Family responsibilities:

Brighton Beach Primary School is committed to educating our students and our wider community. As such, information relating to eSafety and digital technologies will be produced and distributed through school newsletters and the school website. Information sessions, which may include guest speakers, will be made available to the wider school community at times, which will be advertised through the usual methods of communications.

All students and parents will annually sign an Acceptable Use Agreement. Brighton Beach Primary School will have two forms of the Acceptable Use Agreement, one for use with the Foundation - Year 2 students and one that will be appropriate for the Year 3 - 6 students. Year 3 – 6 will also sign a 1:1 iPad program Acceptable Use Agreement.

All staff members and parents are responsible for ensuring that students adhere to the Acceptable Use Agreement. Any breaches of this agreement will be documented, and appropriate follow up, as set out in the agreement, will occur.

**Safe and appropriate use of digital technologies**

Digital technologies, if not used appropriately, may present risks to users' safety or wellbeing. At Brighton Beach Primary School, we are committed to educating all students to use digital technologies safely, equipping students with the skills and knowledge to navigate the digital world.

At Brighton Beach Primary School, we:

- use online sites and digital tools that support students' learning, and focus our use of digital technologies on being learning-centred
- use digital technologies in the classroom for specific purpose with targeted educational or developmental aims
- supervise and support students using digital technologies for their schoolwork
- effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students
- have programs in place to educate our students to be safe, responsible and discerning users of digital technologies. These include the school's Social and Emotional Learning program as well incursions from external providers such as Project Rockit and Life Education.
- educate our students about digital issues such as privacy, intellectual property and copyright, and the importance of maintaining their own privacy and security online
- actively educate and remind students of our Student Wellbeing and Engagement Policy that outlines the school's values and expected student behaviour, including online behaviours

- have an Acceptable Use Agreement outlining the expectations of students when using digital technologies for their schoolwork
- use clear protocols and procedures to protect students working in online spaces, which includes reviewing the safety and appropriateness of online tools and communities and removing offensive content at the earliest opportunity
- educate our students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and other digital technologies
- provide a filtered internet service at school to block access to inappropriate content
- refer suspected illegal online acts to the relevant law enforcement authority for investigation
- support parents and carers to understand the safe and responsible use of digital technologies and the strategies that can be implemented at home through regular updates in our newsletter, information sheets, website/school portal and information sessions.

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.

A full list of obligations which users of digital technology at Brighton Beach Primary School must abide by are listed in Appendix A.

Information on supervision arrangements for students engaging in digital learning activities is available in our Yard Duty and Supervision Policy.

**Social media use**

Our school follows the Department's policy on Social Media Use to Support Learning to ensure social media is used safely and appropriately in student learning and to ensure appropriate parent notification occurs or, where required, consent is sought. Where the student activity is visible to the public, it requires consent.

In accordance with the Department's policy on social media, staff will not 'friend' or 'follow' a student on a personal social media account, or accept a 'friend' request from a student using a personal social media account unless it is objectively appropriate, for example where the student is also a family member of the staff.

If a staff member of our school becomes aware that a student at the school is 'following' them on a personal social media account, Department policy requires the staff member to ask the student to 'unfollow' them, and to notify the school and/or parent or carer if the student does not do so.

**Student behavioural expectations**

When using digital technologies, students are expected to behave in a way that is consistent with Brighton Beach Primary School Policies: Statement of Values and Philosophy, Student Wellbeing and Engagement Policy, Bully Prevention Policy.

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), Brighton Beach Primary School will institute a staged response, consistent with the policies listed above. School staff are also expected to complete an ICT Incident Report Form (Appendix B).

The school community, as a whole, has a responsibility for the safety of the students at BBPS, and as such, parents and caregivers and others who witness any form of conflict, bullying (including cyber-bullying) or harassment are expected to report this to the school as soon as is practicable.

Breaches of this policy by students can result in a number of consequences which will depend on the severity of the breach and the context of the situation. This includes:

- removal of internet access privileges
- other consequences as outlined in the school's Student Wellbeing and Engagement Policy.

## COMMUNICATION

This policy will be communicated to our school community in the following ways:

- Available publicly on our school website
- Included in staff induction and child safety training processes
- Discussed at staff briefings/meetings as required
- Included in our staff handbook/manual
- Discussed at parent information nights/sessions
- Included as annual reference in school newsletter
- Made available in hard copy from school administration upon request

## POLICY REVIEW AND APPROVAL

| | |
|---|---|
| Policy last reviewed | July, 2022 |
| Consultation | School community via newsletter August 2022<br>School Council – Marketing and Publicity sub-committee August 2022 |
| Approved by | Principal and School Council |
| Next scheduled review date | 2024 |

# APPENDIX A

**User Obligations**

## 1. Authorised Usage

1.1 As the school provides network access, the contents of the school ICT system, including email messages, remain the property of the DET. The school has the capacity to monitor and control the system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.

1.2 All users, whether or not they make use of network facilities and digital technologies on school owned or personal ICT equipment/devices, will be issued with an Acceptable Use Agreement. This document should be read carefully with the acknowledgement page signed and returned to the student's classroom teacher.

1.3 The school's ICT program, including network facilities, communication technologies, and ICT equipment/devices cannot be used until the acknowledgement page of the Acceptable Use Agreement for Internet and Digital Technologies has been signed via Compass.

1.4 The school encourages anyone with a query about these guidelines or the Acceptable Use Agreement for Internet and Digital Technologies to contact the classroom teacher in the first instance.

## 2. Obligations and requirements regarding appropriate use of ICT in the school learning environment

2.1 While at school, using school owned or personal ICT equipment/devices is for educational purposes only.

2.2 When using school or privately owned ICT on the school site or at any school related activity prohibited use includes, but is not limited to, any conduct defined as objectionable and inappropriate that:

- is illegal
- would cause offense to students, teachers or parents, such as profanity, offensive language, obscenity, pornography, unethical or illegal solicitation, racism, sexism
- is derogatory or threatening to another e.g. libellous, slanderous, inflammatory, threatening, harassing; has intention to deceive, impersonate or misrepresent
- has intention to deceive, impersonate or misrepresent
- forwards confidential messages to persons to whom transmission was never authorised by the school, including persons within the school community and persons/organisations outside the school community
- fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus
- breaches copyright
- attempts to breach security and infrastructure that is in place to protect user safety and privacy
- results in unauthorised external administration access to the school's electronic communication
- propagates chain emails or uses groups or lists inappropriately to disseminate information
- inhibits the user's ability to perform their duties productively and without unnecessary interruption, interferes with the ability of others to conduct the business of the school
- involves malicious activity resulting in deliberate damage to school ICT and/or ICT equipment/devices
- involves the unauthorised installation and/or downloading of non-school endorsed software
- breaches the ethos and values of the school.

2.3 In the event of accidental access of such material, authorised user must:

- not show others
- shut down, close or minimise the window
- report the incident immediately to the supervising teacher.

2.4 A person who encourages, participates or otherwise knowingly acquiesces in prohibited us of school, or privately owned communication technologies, on the school site or at any school related activity, may also be found to have engaged in prohibited use.

2.5 While at the school or a school related activity, authorised users must not have involvement with any material, which might place them at risk. This includes images or material stored on privately owned ICT equipment/devices brought onto the school site.

2.6 Authorised users must not attempt to download, install or connect any unauthorised software or hardware onto school ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies that are available. Any authorised users with a query or a concern about this issue must speak with the relevant classroom teacher.

**3. Monitoring by the School**

The school:

3.1 Reserves the right at any time to check work or data on the school's computer network,email, internet, computers and other school ICT equipment/devices, without obtaining prior consent from the relevant authorised user.

3.2 Reserves the right at any time to check work or data on privately owned ICT equipment on the school site or at any school related activity. The authorised user agrees to promptly make the ICT equipment/device available to the school for purposes of any such check and to otherwise co-operate with the school in the process. Before commencing the check, the school will inform the authorised user of the purpose of the check.

3.3 Has an electronic access monitoring system, through Netspace (in accordance with DET requirements), which has the capability to restrict access to certain sites and data.

3.4 Monitors traffic and material sent and received using the school's ICT infrastructures. From time to time this may be analysed and monitored to help maintain an safe digital learning environment.

3.5 From time to time conduct an internal audit of its computer network, internet access facilities, computers and other school ICT equipment/devices, or may commission an independent audit of content and usage.

**4. Copyright, Licensing, and Publication**

4.1 Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Authorised users must not breach laws of copyright, moral right or intellectual property – this includes illegal copies of software, music, videos, images.

4.2 All material submitted for internal publication must be appropriate to the school environment and copyright laws.

**5. Individual password logons to user accounts**

5.1 If access is required to the school computer network, computers and internet access using school facilities, it is necessary to obtain a user account from the school.

5.2 Authorised users must keep usernames and passwords confidential and not share them with anyone else. A breach of this rule could lead to users being denied access to the system.

5.3 Authorised users must not allow another person access to any equipment/device logged in under their own user account. Material accessed on a user account is the responsibility of that user. Any inappropriate or illegal use of the computer facilities and other school ICT equipment/devices can be traced by means of this login information.

5.4 Those provided with individual, class or group email accounts must use them in a responsible manner and in accordance with the Guidelines and Agreement. This includes ensuring that no electronic communications could cause offence to others or harass or harm them, put the owner of the user account at potential risk, contain objectionable material or in any other way be inappropriate in the school environment.

5.5 For personal safety and having regard to Privacy laws, authorised users must not reveal personal information about themselves or others online. Personal information may include, but is not limited to, home addresses and telephone numbers.

**6. Other Authorised User obligations**

6.1 Avoid deliberate wastage of ICT related resources including bandwidth, through actions such as unnecessary printing and unnecessary internet access, uploads or downloads.

6.2 Avoid involvement in any incident in which ICT is used to send or display electronic communication, graphics, audio, video files which might cause offence to others and/or involve objectionable material.

6.3 Abide by copyright laws and obtain permission from any individual before photographing, videoing or recording them.

## 7. Privacy

7.1 School ICT and electronic communication should never be used to disclose personal information of another except in accordance with the school's privacy agreement or with proper authorisation. The Privacy Act requires the school to take reasonable steps to protect the personal information that is held by the school from misuse and unauthorised access. Authorised users must take responsibility for the security of their computer and not allow it to be used by unauthorised persons.

7.2 While after school use of communication technologies by students is the responsibility of parents, school policy requires that no student attending the school may identify, discuss, photograph or otherwise publish personal information or personal opinions about school staff, fellow students or the school. Any such behaviour may result in disciplinary action. The school takes a strong position to protect privacy and prevent personal information and opinion being published over technology networks including Facebook, YouTube, Instagram, TikTok (and any further new technology).

## 8. Social Media & Other Forms of Communication

When using Social Media or other forms of communication, students are expected to ensure that they:

8.1 Respect the rights and confidentiality of others
8.2 Do not impersonate or falsely represent another person
8.3 Do not bully, intimidate, abuse, harass or threaten others
8.4 Do not make defamatory comments
8.5 Do not use offensive or threatening language or resort to personal abuse towards each other or members of the Brighton Beach Primary School community
8.6 Do not post content that is hateful, threatening, pornographic or incites violence against others
8.7 Do not harm the reputation and good standing of Brighton Beach Primary School or those within its community
8.8 Do not upload any film, photography or recorded images of members of the school community without permission of the school.

Note: Use of social media platforms or other forms of communication are not permitted during school time. The decision to use social media platforms outside of school is the responsibility of the parent. The school does not endorse the use of platforms recommended for age groups beyond the primary school setting.

## 9. Procedures for Mobile Phone and Other Electronic Device Use at School

Brighton Beach Primary School accepts that some parents provide their children with mobile phones and other personal electronic devices for communication purposes. Refer to our Mobile Phone Policy for appropriate use of these devices outside of school hours, whilst still on school grounds.

Responsibility:

9.1 It is the responsibility of students who do bring mobile phones or personal electronic devices onto school premises to adhere to the Mobile Phone Policy.
9.2 The school accepts no responsibility for replacing lost, stolen or damaged mobile phones or personal electronic devices. Their safety and security is wholly in the hands of the student.
9.3 The school accepts no responsibility for students who lose or have their mobile phones or personal electronic devices stolen while travelling to and from school.
9.4 It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.
9.5 Students must protect the privacy and dignity of individuals and security of information, to maintain the public standing of the school and compliance with State and Federal laws.
9.6 The school strongly advises that for safety reasons headphones should not be used when students are traveling to and from school, eg. walking, riding a bike, moving on and off buses.

9.7 In accordance with school policies, any mobile phone or personal electronic device being used without teacher permission during the school day will be confiscated.

Parents are reminded that in cases of emergency, the school office remains the appropriate point of contact to ensure your child is reached quickly and assisted in the appropriate way. Students require permission from staff to make a phone call during school time.

APPENDIX B

# BBPS ICT INCIDENT REPORTING PROCESS


## STEP ONE: - Identify Concern

**1. Discuss issue with a colleague or ICT Leader. Identify if the issue involves the following:**

- A student has been EXPOSED to and affected by inappropriate behaviour online. (Including cyberbullying, sexting, exposure to inappropriate material/contact or in breach of school policy).

Or

- A student has ENGAGED in inappropriate behaviour online (including psychological/emotional harm to another student or themselves, engaged in illegal activity or a breach of school policy).

## STEP TWO: - Taking Action - reporting of inappropriate use or incidents

**2. Inquire into the inappropriate behaviour--** This includes discussion with staff/students involved and refer to the school Acceptable Use Agreement for Internet and Digital Technologies/ 1:1 iPad Acceptable Use Agreement/ Student Engagement and Wellbeing Policy /Bullying Prevention Policy as appropriate to identify area of breach.

**3. Report to Leadership-,** inform ICT Leader, Principal/Assistant Principal and fill out the eSmart Incident Report. Depending on the degree of the issue, as determined by leadership::

- Arrange meeting with parents and parties involved, if necessary.

OR

- Contact the parents of all students involved.
- Inform parents outlining inappropriate use of internet/social networking sites and the need for the parents to discuss the incident at home with the child involved.
- Collaboratively determine appropriate consequences as a result of deliberate or inappropriate use.
- If it is an illegal offence, contact relevant authorities. e.g. Victoria Police.

## STEP THREE: Reflection and Wellbeing

**4. Provide well--being support for all staff, students and parents involved in or witness to the incident, as appropriate.**

**5. Debrief on incident with students involved – revisit teaching points, reflect on actions taken, establish future process.**

**6. Check in and monitor.**

# Brighton Beach Primary School
# eSmart Incident Record

| **Name of Student/s** | **Date of Incident** | **Type of Technology/Website involved** |
|---|---|---|
| **Staff involved** | **Where incident occurred** | **Parents informed**<br>**(Phone Call, letter, meeting arranged)** |
| **Type of incident** | | |
| **Other involvement** | | |
| **Response** | | |
| **Resolution/Consequence** | | |
| **Teaching Point/Follow up action** | | |