BRIGHTON BEACH PRIMARY SCHOOL

eSmart & Digital Citizenship Policy & Guidelines

RATIONALE

Digital Technology is changing our world at a rapid rate. Keeping up to date and knowledgeable about all areas of technology can be difficult. However, by developing a culture of ‘Digital Citizens’ where there is a shared understanding of how to act appropriately and responsibly around technology, we are equipping the children of today with skills for tomorrow.

Brighton Beach Primary School (BBPS) has developed the eSmart policy using resources and information from the Victorian Department of Education and Training (DET), Australian Council Media Authority (ACMA) and through guidance from the eSmart program, an initiative of the Alannah and Madeline Foundation. The school has an eSmart committee that has collaborated on developing this policy and procedures. We ask that parents/guardians work in partnership with the school to encourage best practices.

PURPOSE

The aim of the policy is to:

- Establish an eSmart culture, in keeping with the values of the school and the expectations outlined in the BBPS Student Wellbeing and Engagement Policy, which also includes actions and follow through consequences for inappropriate behaviour.
- Educate BBPS students to be smart, safe, responsible and ethical users of digital technologies.
- Recognise that explicitly teaching students about safe and responsible online behaviours is essential in the lives of students and is best taught in partnership between home and school.
- Achieve accreditation as an eSmart school by meeting all criteria as outlined in the eSmart System Tools.

SCOPE

This policy applies to the students, staff and parents of BBPS.

The eSmart Policy should be read in conjunction with the following policy documents:

- Acceptable Use Agreement for Internet and Digital Technologies (P-2 and 3-6)
- Student Wellbeing and Engagement Policy
- Bullying Prevention Policy

DEFINITIONS

See Appendix A for glossary of key terms used in this policy.

POLICY

<u>Staff responsibilities</u>

- All staff members are to be familiar with the above policy documents. 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 education

- Throughout each school year, students will receive explicit education of an eSmart curriculum 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 eSmart curriculum:
  - eSafety – Office of the Children's eSafety Commissioner
  - eSmart School Program – The Alannah and Madeline Foundation
  - Incursions and Excursions, such as Project Rockit.

Family responsibilities

- BBPS is committed to educating our students and also our wider community. As such, information relating to the eSmart Curriculum 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 normal 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 - Year 6 students.

- 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.

Incident reporting

- 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.

- In line with the Bullying Prevention Policy and the Student Engagement and Wellbeing Policy, all students and staff are responsible for reporting any form of bullying (including cyber-bullying) or harassment to either a teacher or member of leadership. School staff will follow the procedures as set out in the above mentioned policy documents **(see also Appendix A).**

User eSmart Obligations

1. Authorised Usage and eSmart Agreement

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 communication 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 class 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 Digital Technologies Acceptable Use Agreement has been signed via Compass consent.

1.4 The school encourages anyone with a query about these guidelines or the Digital Technologies Acceptable Use Agreement to contact the class 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 users 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 use 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 class 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 eSmart 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.
6.3 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 BBPS 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 BBPS 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

BBPS 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.

Breach of Guidelines / Cyber Bullying Management Process

Breaches to the guidelines as set out in this policy will be managed according to the school follow through process, as outlined in the Student Wellbeing and Engagement Policy.

BBPS has developed a process for reporting, responding to, and collecting data in relation to cyberbullying/ bullying and isolated incidents **(see Appendix 2**). Staff and students are explicitly taught this reporting process on an annual basis.

The school has also developed an ethical reporting system of any cyber bullying related incidents – leading staff are to complete this form, to be kept in school records **(see Appendix 3)**

FURTHER INFORMATION AND RESOURCES

See BBPS Website for links to the following relevant policies:

- BBPS Acceptable Use Agreement (Junior and Senior)
- BBPS Bullying Prevention Policy
- BBPS Student Wellbeing and Engagement Policy
- BBPS Student Wellbeing Support Plan
- BBPS Statement of Values
- BBPS Mobile Phone Policy

REVIEW CYCLE

Date Reviewed	October, 2021
Responsible for Review	Principal
Noted at School Council	November, 2021
Review Date	2023

APPENDIX 1 Glossary of terms used in policy and guidelines

Agreement: the eSmart Agreement, reviewed and consented to by key stakeholders, annually**.**

Authorised user: a person who has signed the eSmart Agreement (or has had it signed on their behalf by a.parent) and is authorised by the school to use school ICT.

Communication technologies: includes, but is not limited to, communication made using ICT equipment/devices such as internet, email, instant messaging, online discussions/surveys and mobile phone activities and related applications.

Cyber-bullying: repeated verbal, physical, social or psychological aggressive behaviour by a person or a group directed towards a less powerful person or group that is intended to cause harm, distress or fear, communicated through a device or online platform (refer to Bully Prevention Policy).

Cyber-risks: factors that can contribute to or provide a platform for cyber-bullying or harm. These include un-supervised use of internet, social media platforms, such as, Snapchat, Facebook, Instagram, TikTok and Twitter and online marketing campaigns that promise prizes in return for personal details. Other cyber-risks include, stranger danger, inadvertently downloading viruses, hacking, insecure passwords and posting personal photos online. Tools, such as, firewalls, filters and anti-virus software may help reduce cyber-risks.

Cyber safety: the protection of children when they are online. Cyber safety information addresses online dangers to children, such as; exposure to illegal or inappropriate material, stranger danger, identity theft, invasion of privacy, harassment and cyberbullying. We are not talking about computer security, spam or viruses - ACMA, 2013

eLearning: the use of ICT for educational purposes.

Educational purposes: activities that are directly linked to curriculum related learning.

eSmart: the name of the cyber-safety guidelines that are followed at Brighton Beach Primary School to promote the safe, responsible and ethical use of ICT.

ICT: Information and Communication Technologies, including network facilities, communication technologies, eLearning tools and ICT equipment/devices.

ICT equipment/devices: includes, but are not limited to, computers (such as desktops, laptops, tablets), storage devices (such as USB and flash memory devices, CDs, DVDs, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, and any other, similar, technologies as they come into use.

Network facilities: includes, but is not limited to, internet access to files,websites and digital resources via the school network.

Objectionable material: includes,but is not limited to, pornography,cruelty,violence,ormaterial of a discriminatory nature that it islikely to be detrimental to the wellbeing of students or unsuitable to a school environment.

Personal electronic devices: includes, but is not limited to, iPads, handheld gaming consoles (including but not limited to Nintendo DS, PSP Wii U), phones, smart watches, e-readers (including but not limited to Kindle, Kobo) other internet and 5G accessible devices, and any other similar such devices as they come into use.

School: Brighton Beach Primary School.

School ICT: any ICT owned or operated by the school including, but not limited to, network infrastructure, computers, cameras, tablet devices.

School related activity: includes, but is not limited to, an excursion, camp, sporting or cultural event, wherever its location.

Unacceptable student conduct: includes, but is not limited to, malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, non-sanctioned gaming, impersonation/identity theft or copyright infringement.

APPENDIX 2

BBPS ICT INCIDENT REPORTING PROCESS

1. Identify Concern
2. Take Action
3.Well-being

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.**

APPENDIX 3

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** **(Phone Call, letter, meeting arranged)**
Type of incident		
Other involvement		
Response		
Resolution/Consequence		
Teaching Point/Follow up action		