BRIGHTON BEACH PRIMARY SCHOOL

eSmart & Digital Citizenship

Policy & Guidelines

This policy applies to the students, staff and parents of Brighton Beach Primary School (BBPS)

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 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 with us and encourage best practices at home, as partnership between school and home develops greater success.

Aim

The aim of the policy is to:

- Establish an eSmart culture, in keeping with the values and expectations of the school.
- 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.

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

- Acceptable Use Agreement for Internet and Digital Technologies (P-3 and 4-6);
- Student Engagement Policy (includes actions and follow through consequences for inappropriate behaviour); and
- Bullying Prevention Policy

Implementation

- All staff are to familiarise themselves at the beginning of each school year with the above policy documents 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 consequences imposed if incorrect use occurs.

- 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.

- The staff at Brighton Beach Primary School 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.

- Brighton Beach Primary School 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 3 students and one that will be appropriate for the Year 4 - Year 6 students.

- 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.

- In line with the Bullying Prevention Policy and the Student Engagement Policy, students, parents/guardians and staff are responsible for reporting any form of bullying (including cyber-bullying) or harassment to either a teacher or the student welfare coordinator. The teacher or student welfare coordinator will follow the procedures as set out in the above mentioned policy documents.

- The school community as a whole has a responsibility for the safety of the students at Brighton Beach Primary School, and as such, anyone who witnesses any form of conflict, bullying (including cyber-bullying) or harassment is expected to report this to the school as soon as is practicable.

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, 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 and returned to the student's class teacher. Signed Agreements will be filed in a secure place.

1.4 The school encourages anyone with a query about their user eSmart obligations 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 (e.g. setting up a VPN)
- 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 Engaging in prohibited use also includes:

- encouraging others to engage in any prohibited use;
- participating or otherwise knowingly engaging in prohibited use of school, or privately owned communication technologies, on the school site or at any school related activity.

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

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 that issue must speak with the relevant class teacher or subject 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 conducts 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 log-ons 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 this eSmart Policy & Guidelines and Acceptable Use Agreement for Internet and Digital Technologies. 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 Instagram, YouTube, TikTok, Snapchat or Facebook (and any further new technology networks).

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 members of the school community are to social media without express permission of the school.

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. However, whilst on school property and during school excursions and camps, use of mobile phones or personal electronic devices is not permitted by students unless specifically authorised by the Principal or delegate.

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 a vital and appropriate point of contact and can ensure your child is reached quickly, and assisted in the appropriate way. Phone calls home to parents are to be made with a staff member.

Breach of Guidelines / Cyber Bullying Management Process

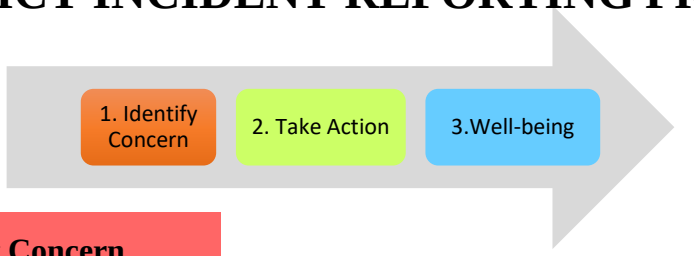
Breaches of this eSmart Policy and Guidelines will be dealt with in accordance with the school Student Engagement Policy.

Brighton Beach Primary School has developed a process for reporting, responding to, and collecting data in relation to cyberbullying/bullying and isolated incidents. This is in the form of a flow-chart. Staff and students have been explicitly taught this reporting process. **See Appendix 1**

The school has also developed an ethical reporting system of any cyber bullying related incidents. **See Appendix 2.**

APPENDIX 1

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 Inclusion Policy/Bullying Prevention Policy for breach of rules and regulations.

3. Report to Leadership, inform ICT Leader, Principal/Assistant Principal and fill out the eSmart Incident Report.

Depending on the degree of the issue 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.
- If it is an illegal offence, contact relevant authorities. e.g. Victoria Police.

**Consequences may be enforced for deliberate, inappropriate use.

Example: Inappropriate website accessed or viewed

- *Report to ICT Leader to have the site blocked*
- *Report to Principal/Assistant Principal if still concerned about impact.*
- *Contact parents of students involved.*

STEP THREE: - Well-being

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

5. Make an explicit teaching point for correct behaviour to students or class involved.

APPENDIX 2

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		

Glossary of terms used in policy and guidelines

a. 'Authorised user' means 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.

b. 'eSmart' refers to the name of the cybersafety guidelines that are followed at Brighton Beach Primary School to promote the safe, responsible and ethical use of ICT.

c. 'ICT' stands for 'Information and Communication Technologies' and includes network facilities, communication technologies, eLearning tools and ICT equipment/devices.

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

e. '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.

f. 'eLearning' refers to the use of ICT for educational purposes.

g. 'ICT equipment/devices' include, 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.

h. 'Agreement' refers to the eSmart Agreement which will be reviewed annually.

i. 'School' means Brighton Beach Primary School.

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

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

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

m. '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.

n. 'Educational purposes' means activities that are directly linked to curriculum related learning.

o. 'Personal electronic devices' includes, but is not limited to, handheld gaming consoles (including but not limited to Nintendo DS, PSP Wii U), MP3 players (including but not limited to iPod, iPod Touch), e-readers (including but not limited to Kindle, Kobo) other internet and 4G accessible devices, and any other similar such devices as they come into use.

p. BULLYING

Definition: Bullying is 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. (Department of Education and Training - Bully Stoppers).

Forms of Bullying:

- Verbal: name-calling, humiliating, sarcasm, put downs, belittling, verbal threats or demands based on culture, race, religion, gender or physical appearance.
- Non-verbal threatening, humiliating or intimidating gestures, facial expressions and body language
- Psychological: stalking or using threatening facial expressions.
- Social: excluding or ignoring others, spreading rumours.
- Cyber-bullying: harassing, excluding or cyber-stalking via SMS messages, mass emailing, chat rooms, blogs, message boards, social networks.
- Physical: hitting, tripping, poking, kicking a student or stealing, taking, damaging or defacing their belongings, harmful actions targeting medical conditions such as allergies.
- Sexual harassment: suggestive comments or gestures, unwelcome advances or conduct of a sexual nature.

q. CYBERSAFETY

"Cybersafety refers to the protection of children when they are online. Cybersafety 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.

r. CYBER-RISKS

Cyber-risks are 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 and TikTok 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.

Other related policies and resources

See BBPS Website for links.

- BBPS Acceptable Use Agreement (Junior and Senior)
- BBPS 1:1 iPad Acceptable Use Agreement (Year 4-6)
- BBPS Bullying Prevention Policy
- BBPS Student Engagement Policy
- BBPS Student Wellbeing Support Plan
- BBPS Statement of Values

Evaluation:

Approved By	School Council
Approval Authority (Signature & Date)	
Date Reviewed	Nov, 2019
Responsible for Review	Education and Policy Sub-Committee
Review Date	Nov, 2021
References	