Cyber-Safety at Brighton Primary School

2022 Cyber-Safety Use Agreement for Students

Dear Parent/Caregiver,

Please sign the Use Agreement Form to ensure you and your child understand the roles and responsibilities required to be Cyber-Safe. 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.

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 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. All students will be issued with a Use Agreement and once signed and 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.

While every reasonable effort is made by schools and the Department for Education's administrators to prevent children'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, the Department cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child.

Strategies to help keep Brighton Primary School Cyber-Safe

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices 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.

Parent/Guardian responsibilities include:

1. Discussing the information about cyber-safety with my child and explaining why it is important
2. Supporting the school's cyber-safety program by emphasising to my child the need to follow the cyber-safety strategies
3. Contacting the Principal or nominee to discuss any questions I may have about cyber-safety and/or this Use Agreement

Name of Parent/Caregiver/Legal Guardian _____

Signature of Parent/Caregiver/Legal Guardian _____**Date** _____

https://d.docs.live.net/6522895253aad3e6/BPS ICT Committee/2021-08-30 - Cyber-Safety Use Agreement for Students.docx

(08) 8296 3614
brightonps.info@schools.sa.edu.au

brightonps.sa.edu.au
blog.brightonps.sa.edu.au

1 Highet Avenue
Brighton SA 5048

Government of South Australia
Department for Education

Student responsibilities include:

☐ 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.

☐ I will use the computers and other ICT equipment only for my learning.

☐ I will go online or use the Internet at school only when a teacher gives permission and an adult is present.

☐ If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.

☐ I will log on only with my own user name. I will not allow anyone else to use my name.

☐ I will keep my password private.

☐ I will use the Internet, e-mail, mobile phones, smart watches 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.   Consequences for breaches will be inline with the Mobile Phone and Smart Watch Policy.

☐ I will not post photos of myself or others in school uniform or on school grounds.

☐ I will only use Office 365 for school work purposes, and will not use it to store or share any sensitive or personal information.

☐ While at school, I will:
  · attempt to search for things online that I know are acceptable at our school.
  · report any attempt to get around or bypass security, monitoring and filtering at our school.

☐ If I find anything that upsets me, is mean or rude, or that I know is not acceptable at our school, I will not show others, I will:
  · turn off the screen
  · get a teacher straight away.

☐ The school cyber-safety strategies apply to any ICTs at school.

☐ I will ask permission before I put any personal information online. Personal identifying information includes any of the following:

· my full name	· my phone numbers	· My school name and/or
· my address	· photos of me and/or	year level
· my e-mail address	people close to me.	

☐ I will respect all school lCTs 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.

☐ If I do not follow cyber-safety 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 personal items for potential examination. Such actions may occur even if the incident occurs off-site and/or out of school hours. Consequences will be in line with the schools Behaviour Education Policy.

Name of Student _____**Class** _____

Signature of Student _____**Date** _____

Important Terms

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

'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, chat room discussion groups, 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, 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, smart watches, 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 (e.g. Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

https://d.docs.live.net/6522895253aad3e6/BPS ICT Committee/2021-08-30 - Cyber-Safety Use Agreement for Students.docx

(08) 8296 3614
brightonps.info@schools.sa.edu.au

brightonps.sa.edu.au
blog.brightonps.sa.edu.au

1 Highet Avenue
Brighton SA 5048

Government of South Australia
Department for Education