BRIGHTON STATE SCHOOL

Network Usage and Access Agreement

***Student**:*

I understand that the school's information and communication technology (ICT) services, facilities and devices provide me with access to a range of essential learning tools, including access to the internet. I understand that the internet can connect me to useful information around the world.

While I have access to the school's ICT services, facilities and devices: I will use it only for educational purposes; I will not undertake or look for anything that is illegal, dangerous or offensive; and I will not reveal my password or allow anyone else to use my school account.

Specifically in relation to internet usage, should any offensive information appear on my screen I will close the window and immediately inform my teacher quietly, or tell my parents/guardians if I am at home.

If I receive any inappropriate emails at school I will tell my teacher. If I receive any at home I will tell my parents/guardians.

When using email or the internet I will not:

- reveal names, home addresses or phone numbers – mine or that of any other person
- use the school's ICT service, facilities and devices (including the internet) to annoy or offend anyone else.

I understand that my online behaviours are capable of impacting on the good order and management of the school whether I am using the school's ICT services, facilities and devices inside or outside of school hours.

I understand that if the school decides I have broken the rules for using its ICT services, facilities and devices, appropriate action may be taken as per the school's Student Code of Conduct, which may include loss of access to the network (including the internet) for a period of time.

I have read and understood this statement and the Student Code of Conduct.

I agree to abide by the above statement.

Please note: Children from Prep to Year 3 inclusively are exempt from signing the student section below.

_____ (Student's name)

_____ (Student's signature)

_____ (Date)

***Parent or Guardian**:*

I understand that the school provides my child with access to the school's information and communication technology (ICT) services, facilities and devices (including the internet) for valuable learning experiences. In regards to internet access, I understand that this will give my child access to information from around the world; that the school cannot control what is available online; and that a small part of that information can be illegal, dangerous or offensive.

I accept that, while teachers will always exercise their duty of care, protection against exposure to harmful information should depend upon responsible use by my child. Additionally, I will ensure that my child understands and adheres to the school's appropriate behaviour requirements and will not engage in inappropriate use of the school's ICT services, facilities and devices. Furthermore, I will advise the school if any inappropriate material is received by my child that may have come from the school or from other students.

I understand that the school is not responsible for safeguarding information stored by my child on a departmentally-owned student computer or mobile device.

I understand that the school may remotely access the departmentally-owned student computer or mobile device for management purposes.

I believe _____ (name of student) understands this responsibility, and I hereby give my permission for him/her to access and use the school's ICT services, facilities and devices (including the internet) under the school rules. I understand where inappropriate online behaviours negatively affect the good order and management of the school, the school may commence disciplinary actions in line with this user agreement or the Student Code of Conduct. This may include loss of access and usage of the school's ICT services, facilities and devices for some time.

I have read and understood this statement and the Student Code of Conduct.

I agree to abide by the above statement.

_____ (Parent/Guardian's name)

_____ (Parent/Guardian's signature)

_____ (Date)

The Department of Education through its Information privacy and right to information procedure is collecting your personal information in accordance with the *Education (General Provisions) Act 2006* (Qld) in order to ensure:

- appropriate usage of the school network
- appropriate usage of personal mobile devices within the school network.

The information will only be accessed by authorised school employees to ensure compliance with its Information privacy and right to information procedure. Personal information collected on this form may also be disclosed to third parties where authorised or required by law. Your information will be stored securely. If you wish to access or correct any of the personal information on this form or discuss how it has been dealt with, please contact your child's school. If you have a concern or complaint about the way your personal information has been collected, used, stored or disclosed, please also contact your child's school.

Advice for state schools on acceptable use of ICT services, facilities and devices

ICT and the curriculum

Students use ICT as an integral part of their learning and to equip them to live and work successfully in the digital world. In the Prep to Year 10 Australian Curriculum in all learning areas, students develop capability in using ICT for tasks associated with information access and management, information creation and presentation, problem-solving, decision-making, communication, creative expression and empirical reasoning. This includes conducting research, creating multimedia information products, analysing data, designing solutions to problems, controlling processes and devices, and supporting computation while working independently and in collaboration with others.

Students develop knowledge, skills and dispositions around ICT and its use, and the ability to transfer these across environments and applications. They learn to use ICT with confidence, care and consideration, understanding its possibilities, limitations and impact on individuals, groups and communities.

Student access to the department's ICT services, facilities and devices

The department's *Digital Strategy 2019-2023* supports the investment in new foundations for contemporary learning, with near-seamless access to information and digital technologies at any time, any place and on any device. Essential tools for providing these innovative educational programs include the intranet, internet, email and network services (such as printers, display units and interactive whiteboards) that are available through the department's ICT network. These technologies are vital for the contemporary educational program provided in schools.

At all times students, while using these ICT services, facilities and devices, will be required to act in line with the requirements of the Student Code of Conduct and any specific rules of their school. In addition, students and their parents should:

- understand the responsibility and behaviour requirements (as outlined by the school) that come with accessing the department's ICT services and network facilities
- ensure they have the skills to report and discontinue access to harmful information if presented via the internet or email
- be aware that:
  - access to ICT services, facilities and devices provides valuable learning experiences for students and supports the school's teaching and learning programs
  - ICT services, facilities and devices should be used appropriately as outlined in the Student Code of Conduct
  - the school is not responsible for safeguarding information saved/stored by students on departmentally-owned student computers or mobile devices
  - schools may remotely access departmentally-owned student computers or devices for management purposes
  - students who use a school's ICT services, facilities and devices in a manner that is not appropriate may be subject to disciplinary action by the school, which could include restricting network access

- illegal, dangerous or offensive information may be accessed or accidentally displayed despite internal departmental controls to manage content on the internet
- teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student

- any inappropriate images/footage posted by individuals on website/s is managed according to the Online incident management guideline for school leaders (DoE employees only).

School-specific ICT responsible use procedure

The Use of ICT systems procedure provides direction to school principals around formulating a school procedure on access to the department's/school's ICT services, facilities and devices for parents and/or students to understand and acknowledge. This may take the form of a procedure, policy, statement or guideline and may require consultation with the school community. Acknowledging through signing seeks to support an understanding of what is lawful, ethical and safe behaviour when using or accessing the department's network and facilities by students and their parents. Principals may seek sign-off either on enrolment of students or alternatively at the start of each school year. Students should be reminded of their responsibilities at the beginning of each school year.

The following dot points are to assist schools to formulate their own procedure. Further guidance on drafting this section can be sought from the Use of ICT facilities and devices guideline.

Purpose statement

- Information and communication technology (ICT), including access to and use of the internet and email, are essential tools for schools in the provision of innovative educational programs.
- Schools are constantly exploring new and innovative ways to incorporate safe and secure ICT use into the educational program.

Authorisation and controls

The principal reserves the right to restrict student access to the school's ICT services, facilities and devices if access and usage requirements are not met or are breached. However restricted access will not disrupt the provision of the student's educational program. For example, a student with restricted school network access may be allocated a stand-alone computer to continue their educational program activities.

The Department of Education monitors access to and use of its network. For example, email and internet monitoring occurs to identify inappropriate use, protect system security and maintain system performance in determining compliance with state and departmental policy.

Responsibilities for using the school's ICT facilities and devices

- Students are expected to demonstrate safe, lawful and ethical behaviour when using the school's ICT network as outlined in the Student Code of Conduct.
- Students are to be aware of occupational health and safety issues when using computers and other learning devices.
- Parents/guardians are also responsible for ensuring students understand the school's ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements.
- The school will educate students (DoE employees only) regarding cyber bullying, safe internet and email practices, and health and safety regarding the physical use of ICT devices. Students have a responsibility to adopt these safe practices.

- Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so that it cannot be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students).
- Students cannot use another student's or staff member's username or password to access the school network. This includes not browsing or accessing another person's files, home or local drive, email or accessing unauthorised network drives or systems. Additionally, students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Students need to understand that copying software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from enforcement agencies.

Acceptable/appropriate use/behaviour by a student

It is acceptable for students while at school to use the school's ICT facilities and devices for:

- assigned class work and assignments set by teachers
- developing appropriate literacy, communication and information skills
- authoring text, artwork, audio and visual material for publication on the intranet or internet for educational purposes as supervised and approved by the school
- conducting general research for school activities and projects
- communicating or collaborating with other students, teachers, their parents or experts in relation to school work
- accessing online references such as dictionaries, encyclopaedias, etc.
- researching and learning through the department's eLearning environment

Unacceptable/inappropriate use/behaviour by a student

It is unacceptable for students while at school to:

- use a device in an unlawful manner
- download, distribute or publish offensive messages or pictures
- use obscene, inflammatory, racist, discriminatory or derogatory language
- use language and/or threats of violence that may amount to bullying and/or harassment, or stalking
- insult, harass or attack others or use obscene or abusive language
- deliberately waste printing and internet resources
- damage computers, printers or network equipment
- commit plagiarism or violate copyright laws
- ignore teacher directions regarding the use of social media, online email and internet chat
- send chain letters or spam email (junk mail)
- share their own or others' personal information and/or images which could result in risk to themselves or another person's safety
- knowingly download viruses or any other programs capable of breaching the department's network security
- use in-phone cameras inappropriately, such as in change rooms or toilets
- invade someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material