Acceptable Use of the Network Policy (Students)

1 Purpose

The purpose of this *Acceptable Use of the Network Policy* (Students) (the Policy) is to set out guidelines for acceptable use of the network and Internet by students of Brisbane Girls Grammar School (the School).

2 Scope

This Policy applies to all students who use the School's IT network and services. Compliance with this Policy (and all related documents) is a condition of access to the network and continued permission for a student to use IT services.

3 Policy

In keeping with the intent of the School to provide a quality education for girls, the School provides its students with a technology-rich learning environment, which includes a BYOD program, and access to the Internet and other network resources.

Using the School's wireless connection, network services (the network) and Internet brings with it certain rights and responsibilities, both ethical and legal. It is the aim of the School to protect the rights of each student and to require that each student behaves in a responsible manner.

This Policy aims to ensure that each student understands her rights and responsibilities when using the network, the School's electronic resources and when using her own personal device while connected to the network. The Policy states that the network is provided for the educational benefit of the student and that all students should use the network in a responsible and safe manner.

The terms and procedures of this Policy are outlined in detail in **Appendix A**.

4 Roles and responsibilities

4.1 The Principal (or authorised delegate)

The Principal (or authorised delegate) is responsible for:

(a)   ensuring application of the Policy across the School

(b)   ensuring all students receive instruction in acceptable use of the School's Network

(c)   ensuring all students are aware of the Policy and its content

(d)   establishing a process to ensure adequate supervision is conducted.

4.2 Director of Information Technology

The Director of Information Technology is responsible for:

(a)   monitoring student use of the network

(b)   reporting any unacceptable use to the Principal (or authorised delegate)

(c)   ensuring appropriate network access and restrictions are applied to student access

(d)   assisting with student IT enquiries or concerns.

4.3   Students

Students are responsible for:

(a)   upholding the School's Policy by ensuring their appropriate use of the network via safe, lawful and ethical behaviour

(b)   reporting any breaches of this Policy to a staff member. This may be a class teacher, Head of House or any other Brisbane Girls Grammar School staff member.

5   Review and Monitoring

This Policy shall be reviewed annually or in the event of any information, incident, legislative changes or organisational practice that would demonstrate the need for a review.

Document title	Acceptable use of the network (students)	Author	Deputy Princpal
Version	506.2008.2	Approval	Principal
Distribution	Minerva	Date	August 2022

6   Definitions

BYOD Program means the School's 'Bring Your Own Device' program, which permits a student to bring her own personal device to School, for educational purposes.

IT Services means the information and communications technology services provided or otherwise made available by the School, being:

- the network and portals

- facilitating access to web-based systems, or overall Internet

- connection and access to the above through a personal device.

Network means the School's wireless connection and associated network that is available to students and staff on-campus, at no cost, through secure login.

Personal device means a student's own personal computer device.

Portal means the Learning Management System and Intranet, which provides: access to materials that supports classroom-based learning for each student to download; the ability to submit work; and allows interaction with other students or teachers.

Web-based systems means educational websites and applications that students may be directed to use as part of the curriculum.

7   Related documents

Promoting Positive Relationships Policy

Privacy Policy

Intellectual Property Policy

Copyright Policy

Social Media Policy (Students)

Student Code of Behaviour

1 Responsibility

IT services are made available to students for educational purposes. Any use of IT services by a student other than for these purposes, or in accordance with this Policy, may result in disciplinary action.

Parents are responsible for ensuring their daughter is aware of this Policy and its application to the use of IT services, both at School and (in respect of the Portal and web-based systems) from home. Any use of the Internet for School-based activities or when away from School (which may include web-based systems) is the responsibility of the student's parents.

While the School employs content-filtering technology to limit the websites that may be accessed using the network, these technologies are not foolproof.

2 Network Use

Access to the network is only available to students while on the School campuses.

By accessing the network, students understand and agree that all use may be tracked and recorded by the School. This includes the School monitoring a student's Internet searches (generally via a search engine, such as Google), webpages browsed, content viewed or downloaded and email activity. It is further understood that:

- IT staff and other authorised senior staff may view files and activity logs in the course of their day-to-day duties. If illegal or inappropriate content is discovered on the network or viewed via logs, this activity will be reported to the Principal or other senior staff

- with the Principal or account owner's authorisation, IT staff may be instructed to access a user's email account

- students must keep their network login details (including password) confidential at all times. If a student forgets her password, or suspects that someone else knows her password, she must contact the IT Department to obtain a new password

Appendix A: Network Use

- students must only use the network for curriculum and educational activities

- students must never damage or disable School computers, computer systems or networks

- students must never attempt to circumvent the School's security or content filtering software or protocols. This includes setting up proxies, wireless hotspots or hacking and downloading programs required to enable any of the foregoing.

3 Use of the Portal and Web-based Systems

The portal can be accessed through the network while at School or remotely from home through a student's own Internet connection.

Some of the School's web-based systems are websites and applications provided and hosted by third parties; the content and operation of these systems are not controlled by the School. The use of these websites may be governed by the third party provider's terms of use and students must comply with such terms when using the site. Students may be required to create a login for these websites, which will include the disclosure of their name and School email address.

4 BYOD Program

The School's BYOD Program requires students to bring their own personal device to School to connect to the network, access the portal and use for access to web-based learning programs and other online resources for educational purposes. All students must bring to school at least one personal device that is considered as the primary device to be used for learning. This device must meet the minimum requirements as detailed in the BYOD Program Guidelines. This personal device is to be used in all curriculum areas.

A student's participation in the BYOD Program is subject to the student complying with the terms of this Policy.

If using a personal device at School or during off-campus School-related activities (such as School excursions or sporting events):

- a student is responsible for any activity that is performed on her personal device or using her personal device with her user account that involves accessing the network

- each personal device must have security measures, including password protection for access, screen savers and emails

- regular back-ups (recommended to be at least daily) must be performed of all curriculum and learning-related files on a personal device to an external back-up device or an appropriate School network drive. Students are fully responsible for backing up their data and for any loss of data from a personal device.

The School is not responsible for, and will not accept any claims for damage, loss or theft of, a personal device arising out of a student's use of her personal device. This includes claims for damages to a student's personal device caused by another student or damage from viruses contracted while connected to the Network or other IT systems. The School will not be liable for any loss of data or data corruption, configuration or system settings changed on a personal device.

Parents are responsible for all costs associated with the provision of a personal device, including any software licenses, anti-virus programs, back-up services, insurance and wireless data card or other Internet connection costs. There is no cost for accessing the School network while on the School campus. The School may provide certain software to students for installation and use on personal devices from time to time.

There may be a requirement for students to download and install certain software or other applications on their personal device from time to time to enable access to the IT systems. It is the student's responsibility to maintain the latest versions of this software.

Students must not connect a personal device to the network via an ethernet cable.

For the purposes of this Policy, the 'use' of a personal device is the connection of the personal device to any of the School's IT systems while at School (whether via the network or the student's own Internet/data service) and while away from School. It also includes the use of a personal device in any capacity while on School campus (for

example, to access Internet sites using the student's own Internet connection).

The School will not be responsible for providing maintenance and hardware support for personal devices. The IT Department will, however, endeavour to assist students where possible with technical asssitance with software support, connectivity issues and warranty returns for machines purchased through the School's third party computer supplier.

5 Internet, Online Communication, Email, and Use of Online Collaborative Websites and Forums

A student is responsible for all content she accesses on the Network through her login details.

Students must ensure that any communication through Internet and online communication services (email, social media, etc.) are related to curriculum and educational activities.

Students must:

- be aware that all use of Internet and online communication services can be audited and traced to the accounts of specific users

- not knowingly access inappropriate Internet sites and activities for any purpose, including unauthorised commercial activities, political lobbying, online gambling or any other unlawful purpose. Students must report any inappropriate sites that are accessible via the network to their teacher or another member of staff

- never intentionally access, download, store or distribute offensive material (e.g., pornography and inappropriate pictures, literature, games or videos), unlawful or criminal material or material containing defamatory comments

- never send or publish unacceptable or unlawful material or remarks, including offensive, abusive, bullying, threatening, harassing or discriminatory comments

- never send or publish sexually explicit or sexually suggestive material or correspondence

- never send or publish false or defamatory information about a person or organisation

- never knowingly initiate or forward emails or other messages containing:

  o a message that was sent in confidence

  o a computer virus or attachment that is capable of damaging recipients' computers

  o spam, e.g., unsolicited advertising material, chain letters and hoax emails.

Student email addresses must only be used for education purposes and for communicating between students or between the student and a member of the School's staff. All email correspondence should be undertaken in a respectful manner.

When using online collaborative forums and software at the direction of teaching staff at School, a student must:

- be responsible and only engage in the forums and websites for educational purpose as recommended by her teacher

- be aware that even though staff have, to the best of their knowledge, verified that the site is authentic and provides educational benefits, the site may still pose the risk of online scams

- immediately report any content that is inappropriate or causes concern to her teacher.

It is important that students understand that:

- most email clients are insecure and should be treated as insecure

- most comments and participation in forums is permanent and cannot be removed or revoked

- most software used to operate networks also logs transaction and communications. Email logs and web server logs record information on emails sent and received and on the websites that people visit. Retaining these logs is usually necessary for the maintenance and management of networks and systems.

6   Privacy and confidentiality

Students must at all times respect the privacy of other persons' personal information, including that of other students and staff.

Students must:

- respect and observe all security provisions

- never publish or disclose the name or email address of a staff member or student without that person's explicit permission

- not reveal her own personally identifiable information or that of others including, but not limited to, addresses or location, photographs, credit card details and telephone numbers

- keep passwords/PINs confidential, and change them when prompted, or when known by another user

- never tamper with the files or password/PIN of any other user

- never publish or distribute any material (including screen shots and audio recordings) derived from participating in a video conference unless explicitly authorised by the Principal or her delegate

- never reveal confidential information of the School on any website, forum or by email. This includes, for example, details of School projects.

7   Intellectual property and copyright

Students must respect the intellectual property rights of others and must:

- not use, copy or distribute to others another person's intellectual property (which includes a copyright work, such as an assignment, essay, photograph, software, music, games, video clip or movie) without their permission

- never plagiarise the work of others

- observe the terms of any applicable copyright licence, including acknowledging the author or source of any information used

- ensure any material published on the Internet or Intranet has the explicit approval of the Principal or her delegate and has appropriate copyright clearance.

8 Compliance and Breaches of Acceptable Usage

Students must not use IT systems or any personal device in any way that would breach School rules or policies, including the terms of this Policy or the School's *Student Code of Behaviour*. A student will be held responsible for any breaches caused by allowing any other person to use her account to access the Internet or online communication services not in compliance with this Policy.

Any student who fails to comply with this Policy or otherwise engages in inappropriate conduct may result in disciplinary action.

Students must also be aware that it may be a criminal offence to use an electronic device or telecommunications network to menace, harass or offend another person. Improper use of technology, whether at School, through the network or otherwise may be illegal and expose a student and her parents to civil or criminal legal action. The School may be required or consider it appropriate to notify the appropriate law enforcement body where it becomes aware of any such illegal activity. If this occurs, parents will be notified as soon as reasonably practicable in the circumstances.

9 Further information

For any queries in relation to this Acceptable Use Policy, please contact the Director of IT.

BRISBANE GIRLS GRAMMAR SCHOOL

STUDENT

I understand that Brisbane Girls Grammar School's (**the School**) Information Technology (IT) 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 stored on computers around the world.

Specifically in relation to Internet usage, should any offensive pictures or information appear on my screen I will close the window and immediately inform my teacher in an appropriate manner, or tell my parents/guardians if I am away from the School campus.

If I receive any inappropriate emails at school I will inform my teacher. If I receive any at home, or away from the School campus, I will tell my parents/guardians.

When using email or the Internet I will not:

- reveal personally identifiable information including, but not limited to, home addresses or phone numbers (mine or that of any other person)

- use the School's IT facilities and devices (including the Internet) to offend or cause harm to anyone else.

I understand that my online behaviour is capable of impacting on the good order and management of the School, whether I am using the School's IT facilities and devices inside or outside of school hours.

I understand that if the School decides I have broken the rules for using its IT facilities and devices, appropriate action may be taken, which may include loss of access to the network for a period of time.

I have read and understood this Policy and procedures and I agree to abide by the above rules, in line with the Student Code of Behaviour.

Student Name	Student Signature	Date

PARENT/GUARDIAN

I understand that the School provides my daughter with access to the network, Internet and email to support valuable learning experiences. In relation to Internet access, I understand that this will give my daughter access to information from around the world via IT devices, that the School cannot control what is on those IT devices, and while the School employs content-filtering technology to limit the websites that may be accessed using the network, these technologies are not failsafe.

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

I believe _____ (name of student) understands this responsibility, and I hereby give my permission for her to access and use the School's IT network (including email/Internet) under the rules of the School outlined in this, and related, policies. I understand that students who do not adhere to these rules will be subject to appropriate action by the School. This may include loss of access and usage of the school's IT facilities and devices for some time.

I have read and understood this Policy and procedures and I agree to abide by the above rules.

Parent/Guardian Name	Parent/Guardian Signature	Date