Introduction

In keeping with the intent of the School to provide a quality education for young women Brisbane Girls Grammar School (the School) provides its students with a technology-rich learning environment, which includes a BYOD programme, access to the internet and to other network resources.

Policy

Using the School’s wireless connection and network services (the Network) and the internet bring 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.

In an attempt to protect the students, the School has implemented security features in the Network; one of which is internet-filtering software. No barrier, however, can completely protect an individual, and it is possible that a student might gain access to information which is inaccurate, potentially offensive, defamatory or illegal.

This Acceptable Use Policy – Students has been drawn up in an attempt to ensure that each student understands her rights and responsibilities when using the internet through the Network, the School’s electronic resources and when using her own Personal Device on the Network.

The Acceptable Use Policy states that the Network is provided for the educational benefit of the students. All students should use the Network responsibly and safely.

Related Documents

Other policies that apply to internet and email use at the School include Student Relationships – Rights and Responsibilities, Positive Relationships, Privacy, Intellectual Property, Copyright and Social Media Policy for Students. The Student Code of Behaviour of the School also applies.

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 the Portal
- facilitating access to the Web-based Systems, and
- 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 a secure log-in.

Personal Device means a student’s own personal computer device.

Portal means the GrammarNet Learning Management System (Moodle) and Intranet which provides all manner of materials to support classroom-based learning for each student to download, ability to submit work and interact 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.
Application

This Acceptable Use Policy applies to all students who use the IT 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 the IT Services.

The terms of this Acceptable Use Policy are accepted as part of the Agreement contained in Appendix 1. Each student’s parent/s or legal guardian/s must sign and return the Agreement during enrolment. The policy, as amended from time to time, is available via the Parent Portal.

Responsibility

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

Parents are responsible for ensuring that their daughter is aware of this Acceptable Use Policy and its application to the use of the IT Services, both at School and (in respect of the Portal and Web-based Systems), from home. Any use of the internet when away from School (which may include Web-based Systems) is the responsibility of the student’s parents.

Whilst the School employs content-filtering technology to limit the websites that may be accessed using the Network, these technologies are not failsafe.

Network Use

Access to the Wireless Network is only available to students whilst on the School campus.

In 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, webpages browsed, content viewed or downloaded and email activity. It is further understood that:

ICT 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 is seen via logs, this activity will be reported to the Principal or other senior staff.

On the Principal’s, Deputy Principal’s or account owner’s authorisation, the ICT staff may be instructed to access a user’s email account.

Students must keep their Network log-in details (including password) confidential at all times. If a student forgets her password, or suspects that someone else knows her password, she must contact BGGS IT Services for a new one.

Students must only use the Network for curriculum and educational activities.

Students must never damage or disable computers, computer systems or networks of the School.

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.

Use of the Portal and Web-based Systems

The Portal can be accessed through the Network whilst at School or remotely from home through a student’s own internet connection.

The 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 log-in for these websites, which will include the disclosure of their name and School email address.

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 with Web-based Learning Programs and other on-line resources for educational purposes. All students must own and bring to school at least one Personal Device that is considered as the primary device to be used for learning and must meet the minimum requirements as set out for the BYOD Program. 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 Acceptable Use Policy.

In 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 for the Network
- each Personal Device must have security measures, including password protection for access, screen savers and emails
- regular backups (recommended to be at least daily) must be done of all curriculum and learning related files on a Personal Device to an external backup 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 whilst connected to the Network or other IT Services. 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, back-up services, insurance and 3G wireless data card or other internet connection costs. There is no cost for accessing the School Network whilst on the School campus. The School may provide certain software to students for installation and use on Personal Devices at no cost 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 Services.

Students must not connect a Personal Device to the Network via an Ethernet cable.

For the purposes of this paragraph, the “use” of a Personal Device is the connection of the Personal Device to any of the School’s IT Services whilst at School (whether via the Network or the student’s own internet/data service) and whilst away from School. It also includes the use of a Personal Device in any capacity whilst 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 Services Department will however endeavour to assist students where possible with technical support including software support, connectivity issues and warranty returns for machines purchased under the portal.

**Internet, online communication, email, and use of online collaborative websites and forums**

A student is responsible for all content accessed by her using the Network through her log-in 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, unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose. Students will report any inappropriate sites that are able to be accessed through the Network to their teacher or another member of staff
- never intentionally access, download, store or distribute offensive material (e.g. pornography, 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
Acceptable Use Policy - Students

• 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:
  • a message that was sent in confidence
  • a computer virus or attachment that is capable of damaging recipients’ computers
  • 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 School staff. All email correspondence should be in a respectful manner.

When using online collaborative Web2.0 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 the staff has to the best of his/her knowledge verified that the site is authentic and provides educational benefits, the site may still pose the risk of online scams, and
• immediately report any content that is inappropriate or makes her uncomfortable to her teacher.

It is important that students understand that:
• most email is insecure and should be regarded as insecure
• most comments and participation in web2.0 forums is permanent and cannot be removed or revoked
• most software used to operate networks log 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.

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 personal information or that of others, including names, 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 reveal confidential information of the School on any website, forum or by email. This includes, for example, details of School projects.

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
Acceptable Use Policy - Students

- never plagiarise the work of others
- observe the terms of any applicable copyright licence, including acknowledging the author or source of any information used, and
- ensure any material published on the internet or intranet has the explicit approval of the Principal or her delegate and has appropriate copyright clearance.

**Compliance and Breaches of Acceptable Usage**

Students must not use the IT Services or any Personal Device in any way that would breach School rules or policies, including the terms of this Acceptable Use Policy or the Code of Behaviour of the School. 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 Acceptable Use 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.

**Further information**

For any queries in relation to this Acceptable Use Policy, please contact the Director of ICT.
Appendix 1
Acceptable Use of the Network Policy
Parent/Guardian’s Agreement Form

Agreement

Brisbane Girls’ Grammar School (School)

And

__________________________________ (parent/s name/s) (I/We)

being the parent/s of

___________________________________ (daughter’s name) (my/our daughter)

I/we have read and understood the Acceptable Use– Students Policy governing the use of the Network, Portal, Web-based Systems and her Personal Device by my/our daughter (as those terms are defined in the Acceptable Use Policy).

I/we give permission for my/our daughter to use the Network Portal, Web-based Systems and her Personal Device, and accept the conditions imposed on her by the Acceptable Use Policy.

I/we will ensure that the use of the Network, Portal, Web-based Systems and her Personal Device will not contravene the Acceptable Usage Policy or the Code of Behaviour of the School. I/we understand that if my/our daughter does not abide by the conditions imposed by the Acceptable Usage Policy, some or all of her network and device privileges may be revoked, and that she may face further disciplinary action.

I/we also understand and agree that the School may access student usage records, emails and files if the Principal or her delegate believes that there is a Duty of Care issue or a breach of the Acceptable Use Policy. I/we consent to the collection, use and disclosure of my/our daughter’s personal information for these purposes, in accordance with the School’s Privacy Policy.

I/we understand that the Acceptable Use Policy is reviewed and up-dated from time to time with the most recent version being available on the School’s Intranet. Material changes to the Acceptable Use Policy will be communicated to me/us by the School. I/we understand that I/we am/are deemed to have accepted any communicated changes to the Acceptable Use Policy where my/our daughter continues to use the Network following such change.

I/we give permission for my/our daughter to use the Web-based Systems for educational purpose as recommended by School staff. I understand that even though staff have to the best of their knowledge verified that these sites are authentic and provides educational benefits, these sites may still pose the risk of online scams and hence my/our daughter and I/we will monitor the usage of these sites when not in School to ensure that the sites are used for educational purpose only and if there is any doubt of its authenticity, will inform the School and remove my/our daughter’s registration from the site/s. I/we understand that my/our daughter may be required to enter her personal details in order to register and use the Web-based Systems, including her name and school email address. I/we give permission for my/our daughter to do so and to use the Web-Based Systems.

I/we give permission for my/our daughter to take her Personal Device to School and to use her Personal Device to connect to the IT Services for educational purposes. I/we understand that I/we are responsible for any loss, damage or theft of
my/our daughter’s Personal Device and for all costs (including service provider charges and insurance) relating to the use of her Personal Device.

Where there is more than one parent/guardian, we each accept full responsibility under this Agreement.

Signed: ____________________________________________       Date: __________________

(Signature of Parent/Guardian)

Signed: ____________________________________________       Date: __________________

(Signature of Parent/Guardian)