BRISBANE GIRLS GRAMMAR SCHOOL

Acceptable Use of the Network Policy (Employees)

1 Purpose

The purpose of this *Acceptable Use of the Network Policy (Employees)* (the Policy) is to detail guidelines for acceptable use of the network and School-provided Internet access by employees of Brisbane Girls Grammar School (the School).

2 Scope

This Policy applies to all employees of the School, as well as other users who have access to the School's network, including the Internet (e.g. volunteers, P&F employees, pre-service teachers, etc.).

3 Policy

The primary purpose for which the School provides access to the network and Internet to its employees is to assist them in carrying out the duties of their employment. They may also use the network or Internet for reasonable private purposes which are consistent with this Policy. They may not use the network or Internet access provided by the School in a way that significantly interferes with the duties of their employment or to expose the School to significant cost or risk of liability.

Details about acceptable and unacceptable use of the network, Internet/email use, Application use, interaction with students and consequences of unacceptable use can be found in **Appendix A**.

4 Roles and responsibilities

4.1 The Principal (or authorised delegate)

The Principal (or authorised delegate) is responsible for:

(a) ensuring the implementation of this Policy in a way that is suitable for the School

(b) establishing a process to ensure adequate supervision of network use is conducted

(c) maintaining School user agreements in consultation with staff in relation to this Policy.

4.2 Director of Information Technology

The Director of Information Technology is responsible for:

(a) monitoring staff use of the network

(b) ensuring all staff/volunteers receive instruction in acceptable use of the network, and are familiar with the content of the Policy

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

(d) ensuring appropriate network access and restrictions are applied to staff access.

4.3 School staff

(a) All staff/volunteers are bound by the Policy for their own use and share supervisory responsibility for students/participants using the services based on the *Acceptable Use of Network Policy (Students)*

(b) Should a staff member or volunteer become aware of unacceptable use by other staff/volunteers, they must refer it immediately to the Principal (or authorised delegate).

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.

6 Definitions

IT means Information and Communication Technologies

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

(a) the Network and the School's Intranet

(b) facilitating access to web-based systems or the broader Internet

(c) connection and access to the above through a Personal Device (under the BYOD Program).

IT facilities and devices include, but are not limited to, computers (including desktops, laptops, netbooks, handheld devices, PDAs, iPads and other tablets, iPods, wearable devices, eBook readers and peripheral devices such as monitors, keyboards and mice), telephones (including mobile phones), removable media (such as USBs, DVDs, Blu-rays and CDs), radios or other high-frequency communication devices (including microphones), televisions, digital or analogue players and records (including DVD, Blu-ray and video), cameras, photocopiers, facsimile machines, printers (and other imaging equipment such as scanners), interactive whiteboards, projectors and screens, videoconferencing and teleconferencing devices.

IT network and systems includes electronic networks, servers, switches, the Internet, email, webmail, social media, fee-based web services, school application and other locally hosted software applications.

Personal electronic devices includes all types of mobile and smart phones, laptops, tablets, cameras and video recorders, hand-held game devices, music devices, wearable devices, USBs, PDAs, eBook readers, other palm and handheld devices and other equipment, as determined by the School.

Email means the School-provided electronic mail systems and computer accounts.

Messaging includes, but is not limited to, calendar and scheduling programs, chat sessions, Skype for Business, Microsoft Teams, newsgroups and electronic conferences.

Videoconferencing includes but is not limited to Zoom, Microsoft Teams and Skype for Business.

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 login.

7 Related documents

Social Media Policy (Staff)

Photography and Filming Policy

Copyright and Intellectual Property Policy

Workplace Bullying Policy

Anti-Discrimination Policy

Sexual Harassment in the Workplace Policy

Records Management Policy

BRISBANE GIRLS GRAMMAR SCHOOL

Appendix A: Network Use

1 What is acceptable use?

Subject to the balance of this Policy, employees may use the network and Internet access provided by Brisbane Girls Grammar School (the School) for:

(a) work-related purposes

(b) sending and receiving personal email messages, provided that if email messages are sent with a School email address in the 'From:' or 'Reply-To:' header, a disclaimer shall accompany the email to the effect that the views of the sender may not represent those of the School (automatically added to outgoing emails sent to external accounts)

(c) reading and posting personal messages (email, online) on the same condition specified above accessing the Internet for personal purposes provided that the personal use is moderate in time, does not incur significant cost for the School and does not interfere with the employment duties of the employee or their colleagues. The utilisation of any other Internet service or network protocol for personal purposes will only be allowed after obtaining permission to do so from Brisbane Girls Grammar School.

2 What is not acceptable use?

The network or Internet access provided by the School may not be used to:

(a) defame, harass, abuse or otherwise offend other Internet and email users, individuals, schools or other organisations

(b) refer to people in a manner that could reasonably be interpreted as being offensive

(c) knowingly access inappropriate Internet sites and activities

(d) 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

(e) create or distribute any form of malicious or harmful material via the Internet or email

(f) attempt to obscure the origin of any message or download material under an assumed Internet address or otherwise disguise the user's identity

(g) knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter such information with malicious intent

(h) infringe copyright or unlawfully circumvent technological protection measures designed to deter copyright infringement

(i) maintain or support a personal private business, including personal commercial purposes

(j) disrupt communication and information or degrade network services by sending unsolicited or unauthorised electronic messages (spamming), other junk email including chain email or other inappropriate use

(k) any illegal purpose

(l) knowingly cause interference with or disruption to any network, information service, equipment or any user thereof

(m) disseminate personal contact information of employees, students or parents of the School without their consent

(n) knowingly cause any other person to view content which could render the School liable pursuant to equal opportunity or sex discrimination legislation at the suit of that person

(o) knowingly download or requesting software or media files or data streams for personal use that the employee has reason

to believe will use a greater amount of network bandwidth than is reasonably appropriate

(p) store personal files or content on a long-term basis, which would have a negative effect on network performance and storage capacities.

It should be noted that this list is not exhaustive and with the changing nature of technology and Internet content there may be other uses (e.g. relating to an undesired impact on the School's *Duty of Care* or reputation which the Principal, at her discretion, may deem to constitute unacceptable use).

3 Internet and email interaction with students (Social Networking)

The following principles apply:

(a) Staff should ensure that they do not communicate with students from a private or personal email address. Communication with students via School email should be for professional or official purposes only.

(b) Staff must not use Internet social networks such as Facebook, Instagram, SnapChat or YouTube, or others to contact or access students enrolled at, or attending, the School.

(c) If staff use social networks in personal time, they must ensure that their accounts are private and that access is restricted to specific people who are not students (or even recent past students).

4 Consequences of unacceptable use

The School will review any alleged breach of this Policy on an individual basis. If the alleged breach is of a very serious nature, which breaches the employee's duty of fidelity to the School (for example, emailing confidential information of the school to another School, contravenes their Duty of Care responsibilities etc.), the employee shall be given an opportunity to be heard in relation to the alleged breach and if it is admitted or clearly established to the satisfaction of the School the breach may be treated as grounds for dismissal.

Activity which the School deems may be illegal will be referred to Queensland Police Service.

Otherwise, an alleged breach shall be dealt with as follows:

(a) initially, the employee shall be informed of the alleged breach, given an opportunity to respond to the allegation, and if it is not satisfactorily explained, be asked to desist from, or where applicable to remedy, the breach

(b) if the breach is not desisted from or remedied, the School may either withdraw the employee's access to network resources and the Internet or provide a first warning to the employee, to which the employee shall have an opportunity to respond

(c) if the infringing conduct continues, the employee may be given a second and a third warning, to each of which they shall have an opportunity to respond

(d) if a breach is committed after the third warning, the employee may be dismissed.

5 Other important information about technology and email use

Staff are urged to think carefully about their use of email to communicate, especially in the context of the School's *Privacy Policy*, confidentiality/security of sensitive information and what constitutes as a record.

(a) Staff must seek permission from the IT Steering Committee or IT Department before installing any new software or hardware onto any School-owned computer or server. Furthermore, staff must also seek permission if they intend to use any externally hosted services or websites to upload student information or student work.

(b) IT staff may be required to access a user's email account. Authorisation for this

action can only be given by the Principal (or her direct delegate) or the account owner.

(c) Most email is insecure and should be regarded as insecure unless it has been encoded or encrypted. Email can be compared to a postcard in that anyone who receives it can read it. Email may also be read by others if it is stored on servers during transmission.

(d) Emails are hard to destroy. Even after you delete an email at your desktop, in most cases it is still recoverable.

(e) Most software used to operate networks, including web servers and gateways, logs transaction and communications. These logs will normally include the email addresses of senders and recipients of email at the time of transmission. The content of emails themselves would not normally be logged but may be stored on mail servers. Similarly, web server logs record information on the sites that people visit. The keeping of these logs is usually necessary for the routine maintenance and management of networks and systems. System administrators are also capable of reading the contents of emails sent and received by the corporate network.

(f) Users understand that IT staff may view any 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 to have been accessed by a user, this activity will be reported to the Director of IT for passing to appropriate authorities.

(g) While there is no specific provision dealing with retention of email in Australia, corporations law and various government departments, under the *Archive Act*, may consider emails an official record of the School.

(h) In some circumstances, an email may be considered a binding contract and staff must be careful about any external communications that could be considered an undertaking or commitment on behalf of the School if not authorised to do so.

In using the network and Internet of Brisbane Girls Grammar School, staff acknowledge and agree that such use may result in their personal information being transferred overseas. The School will only transfer personal information of staff overseas where:

(a) the staff member has provided their express consent

(b) the transfer is authorised or required by law

(c) the School has outsourced a business activity or function to an overseas service provider with whom the School has a contractual relationship.

6 Use of videoconferencing technology

The following principles apply:

(a) Use of videoconferencing technology provided by the School and on the School's Network must be for business and professional use only.

(b) Zoom must only be used for classroom content including delivering curriculum, class discussions and group questions

(c) Zoom must not be used for one on one discussions or discussions that could contain sensitive information including personally identifiable information such as individual student or teacher information. Microsoft Teams should be used in these instances.

In addition users should ensure:

(a) They only ever share an intended application rather than their entire screen when sharing screens

(b) They only share document via company approved methods, never via Zoom.

(c) Never utilize free accounts for meetings where participants will discuss confidential or sensitive content.

(d) Cover webcams whenever not in use

(e) Always host a meeting with a unique password