Network Usage Policy

(Including Internet, Email, Social Media and Device Usage)

Policy

The Beehive Montessori School's Network Usage Policy provides guidance on the appropriate use and protection of the School's network systems by all staff, students and visitors. This policy covers the use of all electronic communication including social media, and all devices within the School Network that connect, or have the potential, to connect to the internet.

The School Network includes all software, hardware, computer networks and other technology which the School provides, or makes available for use.

Beehive is committed to ensuring a respectful environment that is safe, positive and supportive for all students and staff. The Beehive Montessori School implements the National Child Safe Organisation Principles through its Child Safe Organisation Framework to underpin all Beehive's policies, procedures, practices and strategies to ensure the provision of an environment where children feel respected, valued, supported and safe from harm, including the online environment.

Background

The School provides internet and email services to facilitate the efficient operation of the School as well as the fulfilment of staff responsibilities and student learning.

The School Network may be used outside of work hours for School related work if the use is consistent with professional conduct and does not contravene this policy.

Everyone who uses the School Network, including connecting to the Network, must comply with this policy and comply with the relevant Code of Conduct.

Implementation

1. Confidentiality

    1.1 All users of the Beehive Network are required to be aware of and comply with the School's Privacy Policy. In particular, that it is inappropriate to disclose confidential information, student data and material of a private nature without prior authorisation from the Board or Principal.

    1.2 In the event of a breach of confidentiality, the Principal must be notified immediately.

2. Passwords and identification

2.1 User identification and passwords help maintain individual accountability.

2.2 Everyone using the School Network must identify themselves honestly and accurately at all times.

2.3 Passwords must be kept confidential and are not to be left unattended or visible to other people.

3. Network integrity

3.1. All users of the Network are required to maintain the integrity of the network and data residing on network facilities, and are responsible for:

3.1.1. locking unattended workstations;

3.1.2. reviewing files to ensure the efficiency of storage space utilised (includes reducing email inbox size and duplicate copies of email attachments);

3.1.3. allowing Administration to perform updates to antivirus, anti-spam, or adware software where appropriate.

3.1.4. establishing precautions that mobile computing devices used for Beehive-related work, whether be it personal or Beehive-issued machines, are guarded against theft or loss; and

3.1.5. reporting non-compliant usage immediately to the Principal or Chair of the Board.

3.2. Users with internet access must not download or install software including commercial off-the-shelf software, adware or freeware without prior consent.

3.3. The School Network and all devices are not to be used for private use.

3.4. The School has installed an internet firewall to ensure the safety and security of its networks. Any user who attempts to disable, defeat or circumvent any School security facility may be subject to dismissal.

4. What is acceptable use?

4.1. Users must not use the School Network for any illegal or inappropriate purpose, including:

4.1.1. downloading, recording, storing, copying or distributing pirated software or data;

4.1.2. online gambling, betting or gaming;

4.1.3. accessing, downloading, saving, storing or transmitting material which is sexually explicit, violent, obscene, offensive or disparaging of others on the basis of gender, race, disability, religion, nationality, sexual orientation, age or marital status;

4.1.4. accessing, downloading, saving, storing, sending, displaying or composing a communication containing material which may offend, humiliate or intimidate another person or may result in another person feeling victimised, undermined of threatened;

4.1.5. disabling or overloading a system or network, or circumventing any system intended to protect the privacy or security of another user or external server;

4.1.6. engaging in commercial activity or advertising not related to the school;

4.1.7. plagiarising or otherwise breaching intellectual property laws and regulations, including making such material available for others to copy;

4.2. Any unacceptable use is to be reported immediately to the Principal or Chair of the Board.

5. The display of sexually explicit content on any part of the school Network or devices is not permitted and in some circumstances will be viewed as grooming behaviour or sexual harassment with serious consequences. The Code of Conduct and Staff Code of Conduct guide outlines the School's response to this type of inappropriate network usage.

6. Monitoring
   6.1. Information passing through or stored on the School Network will be monitored.
   6.2. The School reserves the right to inspect any files and emails created, stored, accessed or disseminated on the School Network to ensure compliance with this policy.
   6.3. Users should have no expectation of personal privacy in their online activities while using School-owned or School-leased equipment or the School Network.

7. Copyright
   7.1. The School retains the copyright to any material posted on the internet by any employee in the course of his or her duties.
8. Usage of personal mobile phones and other internet-connected devices by staff and students
   8.1. Student internet-connected devices should be turned off and stored in bags or lockers; and
   8.2. Staff mobile phones and internet-connected devices should be turned off and stored away, except during personal break times (morning tea and lunch), and even then must still be used accordance with acceptable professional conduct.

9. Social media
   9.1. The use of social media during School hours is not permitted, except for administrative purposes.
   9.2. Users must not make comments on behalf of the School without prior consent, or attribute any communications made in a personal capacity to the School.
   9.3. Social media users must be mindful that comments made in a personal forum may be perceived as representing the School.
   9.4. Private social media use must not impinge on the School's values in any way in accordance with the School's Code of Conduct.

Related Documents and Resources

Privacy Policy

Child Protection Policy

Behaviour Policy

Code of Conduct

Staff Code of Conduct

Student Code of Conduct

Staff Handbook

Volunteer Handbook

Royal Commission Creating Child Safe Institutions

Beehive Montessori School Child Safe Organisation

National Principles for Child Safe Organisations

Approved 12/6/23 by the Board Policy Committee. Next review due 12/6/25