(7) - NETWORK USAGE POLICY
(Including Internet, Email and Mobile Phone Usage)

The Beehive Montessori School's Network Usage Policy provides guidance on
the appropriate use and protection of the school's network systems, and the use
of mobile phones.

Rationale

Beehive provides internet and email services to facilitate the efficient operation of
the school as well as the fulfillment of staff responsibilities.

Occasional personal use is permitted if it is reasonable, responsible and does not
interfere with work performance. The Beehive Network may be used outside of
work hours if the use is consistent with professional conduct and does not
contravene this policy.

Who is covered by this policy?

• Everyone who uses the Beehive Network or brings a mobile phone onto
school premises during school hours must comply with this policy.

What is the Beehive Network?

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

Passwords and identification

• User identification and passwords help maintain individual accountability.
• Everyone using the Beehive Network must identify themselves honestly and
accurately at all times.
• Passwords must be kept confidential and are not to be left unattended or
visible to other people.
• All passwords other than personal access to external websites are to be
recorded in the password register in the Beehive office reception.
Confidentiality

- It is inappropriate to disclose confidential information, student data and material of a private nature without prior authorisation from Beehive’s Board or Principal.

Network integrity

- All users are required to maintain the integrity of the network and data residing on network facilities, and are responsible for taking the initiative to:
  - lock unattended workstations;
  - review files to ensure the efficiency of storage space utilised (includes reducing email inbox size and duplicate copies of email attachments);
  - update antivirus, anti-spam, or adware software where appropriate;
  - perform virus checks or inoculation procedures on incoming attachments or external memory storage equipment;
  - update approved software with the latest stable version as available;
  - establish precautions that mobile computing devices used for Beehive-related work, whether be it personal or Beehive-issued machines, are guarded against theft or loss;
  - report non-compliant usage immediately.

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

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

What is acceptable use?

- Users must not use the Beehive Network for any illegal or inappropriate purpose. This includes:
  - Downloading, recording, storing, copying or distributing pirated software or data;
  - Online gambling, betting or gaming;
  - 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;
  - 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 or threatened;
  o Propagating any virus, Trojan horse or trap-door program code;
  o Disabling or overloading a system or network, or circumventing any system intended to protect the privacy or security of another user or external server;
  o Engaging in commercial activity or advertising not related to the school;
  o Plagiarising or otherwise breaching intellectual property laws and regulations, including making such material available for others to copy.
• The display of sexually explicit content on any Beehive system is a violation of the school’s policy on sexual harassment and may result in immediate dismissal.

Monitoring

• Information passing through or stored on Beehive equipment will be monitored.
• Beehive reserves the right to inspect any files and emails created, stored, accessed or disseminated on its network to ensure compliance with this policy.
• Users should have no expectation of privacy while using Beehive-owned or Beehive-leased equipment.

Copyright

• Beehive retains the copyright to any material posted on the internet by any employee in the course of his or her duties.

Mobile phone usage

• Student mobile phones should be turned off and stored in bags or lockers during school hours.
• Staff mobile phones should be turned off and stored away during school hours except during personal break times (morning tea and lunch), and in accordance with acceptable professional conduct.
• Mobile phones should be taken on off-site activities such as excursions and camps for contact in the event of an illness or emergency only.

Social media

• The use of social media sites during school hours is not permitted, except for administrative purposes.
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.