(7) Network Usage Policy
(Including Internet, Email and Mobile Phone Usage)

The Beehive Montessori School’s Network Usage Policy oversees the effective use of network systems for organisational purposes, as opposed to the use of those same systems for personal use or personal financial gain. Other secondary objectives are to control ‘objectionable material’, and the need for Users to use Beehive’s network responsibly and to perform virus checks on files as appropriate.

Rationale

The School provides Users with Internet access and electronic communications services as required for the performance and fulfillment of job responsibilities. These services are for the purpose of increasing productivity and are not for non-organisational activities.

Occasional, reasonable and responsible personal use of Beehive’s Internet and e-mail services is acceptable, provided that this does not interfere with work performance. These services may be used outside of scheduled hours of work, provided that such use is consistent with professional conduct.

Levels of Responsibility

• Each User using Beehive’s network facilities must identify himself or herself honestly, accurately and completely when setting up accounts. No User must impersonate any other person whilst using network facilities.

• User IDs and passwords help maintain individual accountability for all Beehives’ systems resource usage. Any User who obtains a password must keep that password confidential. Passwords are not to be left unattended or visible to other Users. Passwords relating to school matters (ie all passwords other than personal access to external websites) are to be recorded in the password register in the Beehive office reception.

• Beehive retains the copyright to any material posted on the Internet by any employee in the course of his or her duties.
Levels of Responsibility (cont’d)

• Users are reminded that it is inappropriate to disclose confidential information, student data and/or any material of a private nature without prior authorization from Beehive’s Board or Principal.

  • 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. This includes reducing email inbox size and duplicate copies of email attachments.
    - perform virus checks or inoculation procedures on incoming attachments or external memory storage equipment.
    - not open email attachments from unknown sources in order not to propagate viruses; the proper procedure being to detach the file, store it in a specified local folder and to then scan that folder for possible viruses.
    - update antivirus, anti-spam, or adware software where appropriate.
    - 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.

  • Users with Internet access may not use network facilities to access entertainment content including streaming videos, videos, music or games, playing games over the Internet, or accessing social networking services like FaceBook or LinkedIn, or propagating chain email broadcasts. Beehive retains the right to charge Users at commercial rates for the abuse of network systems.

  • Users must not use Beehive’s network facilities to:
    - download, record, store, copy or distribute pirated software or data.
    - Propagate any virus, Trojan horse or trap-door program code.
    - Disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user or external server.
Levels of Responsibility (cont’d)

9. • Violations of network and Internet use include, but are not limited to, accessing, downloading, uploading, saving, archiving, receiving, recording, editing or sending material that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent, or defamatory language.

10. • The display of any kind of sexually explicit image or document on any Beehive system is a violation of our policy on sexual harassment, and download or display of illegal sexually explicit material may result in immediate dismissal.

11. • Gambling and illegal activities are not to be conducted on Beehive resources.

12. • 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 will be subject to dismissal.

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

14. • Beehive’s Information Systems and Internet facilities must not be used to violate any laws and regulations of Australia, or any other nation.

15. • Mobile phone usage within School hours is not permitted by staff or students unless it is an emergency.

• Infringements of this policy will be investigated on a case-by-case basis.