RESPONSIBLE USE OF INFORMATION COMMUNICATION TECHNOLOGY POLICY

PURPOSE

The Melbourne Montessori School network is provided for staff and students to promote educational excellence by facilitating resource sharing, innovation and communication.

The Responsible Use of Information Communication Technology Policy provides staff and students with the opportunity to utilise these technologies appropriately to enhance teaching and learning in a safe physical and emotional environment. Any technical applications, procedures or processes that interfere with these primary objectives will be considered an infringement of Responsible Use, and therefore unacceptable.

To ensure all members of the Melbourne Montessori School community are accessing and using communication technologies in an acceptable manner in accordance with our Children's Charter and Staff Charter at Melbourne Montessori School, the Behaviour Management Policy, the Responsible Online Behaviour Policy and the law.

SCOPE

This Responsible Use of Information Communication Technology Policy applies to all users of the School network and School owned or leased equipment, and BYO devices connected to the network.

1. Rights and Responsibilities
2. School Network
3. Software and Hardware
4. Copyright
5. Printing
6. Information Technology systems
7. Breach of the Policy

DEFINITIONS

Communication technologies include, but are not limited to, computers and the School network, Internet, mobile phones, wireless devices, personal music devices MP3 players, PDAs, recording devices or portable storage devices, including USB and flash memory devices.

1. Rights and Responsibilities

Members of the Melbourne Montessori School community are expected to comply with the behavioural expectations outlined in the Behaviour Management Policy, Children's Charter, Staff Charter, Privacy Policy and the Responsible Online Behaviour Policy.

2. School Network

The School network is a shared workspace for all staff and students. It provides access to personal and shared work spaces, technologies such as email and internet browsing, and other software applications.

Users of the School network should ensure that they:

- Use only the username and password assigned to them.
- Store files on the system which are relevant to teaching, learning or the efficient administration of the School and organised and managed efficiently by the user.
- Log out when they have finished using the network or are leaving a computer unattended.
- Use email as an electronic communication for educational purposes only. School email accounts are explicitly provided for staff and students for the enhancement of excellence in teaching, learning and administration of the School.
- Do not attempt to access websites or software which has been blocked by the School network security systems.
- Do not access inappropriate material such as Pornographic or adult content, whether stored locally or on the internet, even if it's still accessible behind the internet filter.
- Maintain the integrity of the School network by not attempting to harm the network or other user's data or to delete or modify files on the network or on another person's device.

The School has the right to check any material put on the network, in personal user accounts, if there is a question that it is suitable for use in learning. This includes files saved to personal network space and the content of emails. Privacy will be respected when the accounts are monitored.

3. Software and Hardware

3.1 Users of the School network and computers should be aware that games, music and videos take up a large amount of disk space, risk virus infection and may cause software conflicts. They need to be respectful of the need for others to utilise the networks too.

3.2 All digital equipment will be treated with care and respect.

3.3 Any damage or problems with hardware or software on personal laptops or other digital devices should be reported promptly to teachers and the IT Manager.

3.4 Unsolicited/pirated programs must not be placed on School-owned computers or personal laptops and other computing devices used as part of the BYOD Program.

3.5 All digital equipment, including cameras, iPods, laptops, computers etc. must be stored securely and used appropriately with care and respect for equipment.

3.6 Wireless connected hand held devices may be used for appropriate curriculum activities but must not be switched on or used during lesson times without the direction of the teacher. Teaching staff may use portable devices to facilitate learning by disseminating lesson material via podcasting or other electronic means.

3.7 Access to the internet from a handheld device should only occur via the School network unless directed by a teacher during class time.

4. Copyright

4.1 It is illegal under Australian Law to copy and download or share copyrighted files including: audio, text, video, images and games, if you have not paid for them or received permission to do so.

4.2 Only freeware or shareware software labelled 'public domain' or 'creative commons' may be copied from the School network drives or the internet.

4.3 Copyright Australia has a website that details all copyright information for Australia and overseas. www.copyright.org.au.

5. Printing

5.1 Staff and students must minimise printing at all times by:

- print previewing
- editing on screen rather than on printouts
- selecting double sided/ duplex printing option and
- spell checking before printing

5.2 Staff and students must ensure they only print information that is related to the curriculum and of benefit to their education and learning.

5.3 As a sustainable and environmentally friendly school, staff and students will ensure that they do not waste resources such as unnecessary printing, especially colour printing.

6. Information Technology systems

6.1 The IT staff will regularly undertake virus checks.

6.2 They will regularly monitor student's email and browsing history.

6.3 They may delete files in the Student Share drive at the end of each term/semester to save server space. Files can be saved externally before being deleted.

7. Breach of this policy

Any breach of this policy will be considered by the Principal and will be dealt with on a case by case basis.

REVIEWED: 2019

Linked with:
Children's Charter Critical Incident Policy Family Media Agreement Health and Wellbeing Policy Privacy Policy Responsible Use of Information Communication Technology Policy Responsible Use of Information Communication Technology User Agreement Staff Charter Behaviour Management Policy Code of Conduct