Policy Name	**Computer Usage Policy**
Related Policies and Legislation	Mobile Electronic Devices Policy AISWA Guidelines – Mobile Phones, E-mail and Internet
Policy Category	Behaviour Management
Relevant Audience	All Treetops Community
Date of Issue / Last Revision	02 May 2011 21 May 2015 - JK 27 October 2016
Date Set for Review	October 2019
Person/s Responsible for Review	Treetops Administration

Computer Usage Policy

Purpose

This policy has been developed to assist teachers to put in place school-based processes and procedures that will both protect and inform students in their use of computer services.

This policy sets out the cyber-safety issues, the computer usage guidelines and the security, administration and internal rules which should be observed when using the computer facilities provided by Treetops Montessori School.

Background

Computer services provided to students at Treetops Montessori School will only be used for learning related activities and appropriate usage time limits will be adopted. Treetops Montessori School will make every reasonable effort to provide a safe and secure online learning experience for students when using the School's computers and/or computer services. The School acknowledges that some individuals will use their personal devices (laptops, tablets, smartphones etc.) to access the School's computer services. This policy also applies to that usage. Treetops Montessori School acknowledges that it is not possible to guarantee that students will not be exposed to inappropriate material and students will therefore be educated in the risks associated with some online activities and the need to adopt protective online behaviours.

Scope

This policy applies to all teachers, students and employees of the School using computers and/or computer services at Treetops Montessori School. All staff and students who use these facilities must be aware of the terms of this policy in order to minimise potential damage to themselves, their colleagues, students and the School, which may arise as a result of misuse of computer facilities.

Procedures

Teachers and Student Supervisors must:

- Follow the usage guidelines that form part of this policy.
- Provide appropriate supervision for students using the computer services at school.
- Maintain student passwords in a confidential and secure manner.
- Advise students they should not reveal personal information including names, addresses, financial details, telephone numbers or images (video or photographic) of themselves or others using the School Internet facilities apart from when using their own school gmail addresses.
- Advise students of the need to:
    - be aware of the legal requirements regarding copyright when downloading information,
    - gain permission before electronically publishing users' works or drawings;
    - acknowledge the creator or author of any material published; and
    - observe appropriate copyright clearance including acknowledging the author or source of any information used.
- Instruct students that they must not allow any other person to use their computer account.
- Instruct students that the consequences of misusing the computer services will be withdrawal of access to the computer services.

School Property

The School is the owner of copyright in all email messages created by its students and employees in performing their duties.

Monitoring

- Activities conducted using the School's online services may be logged and accessed for administrative, legal or security purposes.
- From time to time, the contents and usage of email may be examined by the School or by a third party on the School's behalf. This will include electronic communications which are sent to the school or from the school, or internally within the school.
- Email must be structured in recognition of the fact that the School may from time to time have the need to examine its contents.
- The School's computer network is a business and educational tool to be used primarily for these purposes. Users have the responsibility to use these resources in an appropriate, professional and lawful manner.
- All messages on the School's system will be treated as education or business related messages, which may be monitored. No information or document transmitted or stored on the School's network will be treated as private.
- The school may monitor the use of the Internet, both during school or working hours and outside of those hours. This includes sites and content visited and the length of time spent on the Internet
- Emails will be archived by the School as it considers appropriate.

Personal Use of School Internet and Email Facilities

- Staff are permitted to use the Internet and email facilities to send and receive personal messages, provided that such use is kept to a minimum and does not interfere with the performance of work duties or contradict their contract agreement.
- Staff use of the Internet or email for personal purposes is still subject to the same terms and conditions as otherwise described in this Policy.
- Staff are expected to respect the needs of their colleagues and use the Internet and email in a timely and efficient manner.
- It is expected that such minimal personal staff use will be in keeping with all School policies, and will not injure the reputation of the school or cause embarrassment to any community member.
- Excessive or inappropriate use of email or Internet facilities for personal reasons during working hours may lead to disciplinary action.
- Students are <u>not</u> allowed to use the school's internet and email facilities for personal use (including sending and receiving emails, and accessing social media). The consequences of misusing the computer services will be withdrawal of access to the computer services.

Content of Email, Social Media and Web Pages

- Email and social media correspondence will be treated in the same way as any other correspondence; that is as a permanent record which may be read/viewed by persons other than the addressee and which could result in personal or the School's liability.
- Email and social media users and/or the School may be liable for what is said in an email or social media message. Email / social media are neither private nor secret. Messages may be copied, saved, intercepted, archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an email or social media message may be unexpected and extremely widespread.
- The Internet or email should never be used to:
    - Abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other).
    - Send or receive obscene or pornographic material.
    - Injure the reputation of the School or in a manner that may cause embarrassment to the School.
    - Spam or mass email or to send or receive chain mail. (Mass emailing of items such as *Clippings, Little Twigs, permission slips etc.* by the Office to Treetops families is permitted)
    - Infringe the copyright or other intellectual property rights of another person.
    - Perform any other unlawful or inappropriate act.
- In determining whether an email and/or social media message falls within any of the categories listed above, or is generally inappropriate, the School will consider the response and sensitivities of the recipient of an email or social media message rather than the intention of the sender.
- If inappropriate material is received by email or social media it should be deleted immediately and not forwarded to anyone else. The sender should be discouraged from sending further material of that nature.
- Comments that are not appropriate in the workplace or school environment are also inappropriate when sent by email or social media. Email and social media messages can easily be misconstrued and therefore words and attached documents should be carefully chosen and expressed in a clear professional manner.
- Use of the School's computer network in a manner inconsistent with this policy or in any other inappropriate manner, including but not limited to use for the purposes referred to in point 3 of *Content*, will give rise to disciplinary action.

Privacy

- Staff and students may have access to, or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers. Email and social media messages should not be used to disclose personal information of another except in accordance with the School's Privacy Policy or with proper authorisation.
- The Privacy Act requires the user and the School take reasonable steps to protect the personal information that is held from misuse and unauthorised access. Do not allow computers and computer facilities to be used by unauthorised parties, which specifically includes anyone who is not an employee or student of the School. (unless a Confidentiality Agreement is signed)
- Each classroom, staff member and upper primary and secondary student will be assigned a log-in code and password to use the School's computers. It is the individual or classroom teachers' responsibility to ensure that these details are not disclosed to anyone else, except the designated IT Coordinator position documents this information and keep it secure.
- Users are required to log-out when leaving the desk. This will avoid others gaining unauthorised access to personal information, the information of others and confidential information within the School.
- In order to comply with the School's obligation under the Privacy Act, users are encouraged to use the blind copy option when sending email to multiple recipients where disclosure of those person's email addresses will impinge upon their privacy.
- In addition to the above, you should familiarise yourself with the National Privacy Principles and ensure that your use of email does not breach the Privacy Act or the National Privacy Principles.

Distribution and Copyright

- When distributing information over the School's computer network to third parties outside the School, you must ensure that you and the School have the right to do so, and that you are not violating the intellectual property rights of any third party.
- If you are unsure of whether you have sufficient authorisation to distribute information, contact the office personnel.
- In particular, copyright law may apply to the information you intend to distribute and must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through email without specific authorisation to do so.

Encryption and Confidentiality

- When email and/or social media messaging are sent from the School to the network server and then on to the Internet, the information (including message content, contact addresses and IP address etc.) may become public. Encryption will reduce the risk of third parties being able to access such information and should be used in cases where you feel additional security is required. If you require more information in relation to encrypting messages contact the IT Coordinator.
- Items of highly confidential or sensitive nature must be marked CONFIDENTIAL.
- There is a possibility that information sent over the Internet may arrive truncated, scrambled, or may be sent to the wrong address. Where outgoing information is important or urgent, you should verify that the recipient has received the information in its entirety.
- Ensure that all emails sent from your email address contains the School's standard disclaimer message – which read as follows: *The contents of this email are confidential. Any unauthorised use of the contents is expressly prohibited. If you have received this email in error, please advise by telephone immediately and then delete/destroy the email and any printed copies. Thankyou.*

- There is a risk of false attribution of email. Software is widely available by which email messages may be edited or 'doctored' to reflect an erroneous message or sender name. The recipient may therefore be unaware that he or she is communicating with an impostor. Accordingly, you should maintain a reasonable degree of caution regarding the identity of the sender of incoming email. You should verify the identity of the sender by other means if you have concerns.

Downloads

- Downloads are not to occur without teacher or IT Administrator's permission.

Viruses

- All external files and attachments must be virus checked using scanning software before they are accessed. The downloading of infected information from the Internet is potentially fatal to the School computer network.
- A document attached to an incoming email may have an embedded virus.
- Virus checking is done automatically through the network's virus protection software installed on the network server. If you are concerned about an email attachment, or believe that it has not been automatically scanned for viruses contact the IT Coordinator.

The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's email and Internet facilities. You are encouraged to act with caution and take into account the underlying principles intended in the Policy. If you feel unsure of the appropriate action relating to use of email or the Internet you should contact the Administrator.

TEACHER GUIDELINES FOR COMPUTER USAGE

It is recommended that teachers:

- Are aware of their responsibilities for supervising student use of computer services as laid out in this policy.
- Limit the amount of computer usage by students each day, as appropriate to their age.
- Maintain an informed view of the relative risks and educational benefits of online activity by their students. A variety of resources are available from NetAlert (http://www.netalert.gov.au) to assist with this including wall charts, quick reference guides and detailed background information;
- Ensure that students are aware of the possible negative consequences of publishing identifying information online including their own or other students' images;
- Student images or any student-identifying information may only be published via the Director of Communications.
- Check that any material planned for publication on the Internet has the approval of the principal and has appropriate copyright and privacy clearance
- Are aware of the steps to take and advice to give if students notify them of inappropriate or unwelcome online activity by fellow students or members of the public. Such steps may include:
    - collecting as much information as possible about the incident including copies of communications;
    - emphasising to the student that the event is not necessarily their fault;
    - identifying any risky behaviours on the part of the reporting student, and
    - if the incident warrants further attention, escalate it to the Principal. (If you suspect the law may have been broken, such as a possible attempt by an adult to groom or encourage the student to meet face-to-face the Principal will facilitate the need to report this to the appropriate authorities.)

Student Guidelines for Computer Usage

- All computer usage and all communication using online services must be related to learning or school activities.
- Keep your passwords confidential.
- Never knowingly allow others to use your computer account unless directed to by a teacher for the purposes of collaborative learning.
- Log off at the end of each session to ensure that nobody else can use your account.
- Do not send or publish unacceptable or unlawful material or remarks including offensive, abusive, defamatory or discriminatory comments.
- Do not attempt to access inappropriate material.
- Do not engage in any bullying, intimidation or other inappropriate behaviour online.
- Ask a staff member's advice if another user is seeking excessive personal information, asks to be telephoned, offers gifts by email or wants to meet you.
- Immediately tell a teacher if you receive a computer virus or a message that is inappropriate or makes you feel uncomfortable.
- Never knowingly initiate or forward emails containing:
    - A message that was sent to you privately.
    - A computer virus or attachments that are capable of damaging recipients' computers.
    - Chain letters and hoax emails.
    - Spam like unsolicited advertising material, or mail unrelated to learning.
- Be aware that emails and/or social media messages sent or received via the School computers may be audited and traced to your account.t
- Do not damage or disable computers, computer systems or networks of the School.