OSTA
Ottawa Student Transportation Authority

Procedure: Use of Computers, Email, and Internet

Effective Date: October 15, 2011

Approved by: General Manager

Procedure	Number of Pages	Date(s) of Amendment
Use of Computers, Email, and Internet	1 of 3	
Cross Reference Use of Computers, Email, and Internet Policy		
Related Forms		

Procedure

1. Users are required to formally acknowledge their understanding of and agreement with OSTA's Use of Computers, Email, and Internet policy. Formal agreement will be facilitated by agreeing to abide by the terms and conditions as described below.

2. Users will not transmit, relay, or receive information or materials that are threatening, racist, pornographic, or that are malicious, inappropriate, and/or unlawful. Note that e-mail constitutes a legal document. Existing laws for libel and/or defamation of character apply. Email is also subject to legal subpoena.

3. All users acknowledge their rights and responsibilities by becoming familiar with the OSTA Policy: Use of Computers, Email, and Internet. OSTA has the right to monitor the individual uses of its technology. To facilitate regular planning and reporting, OSTA does monitor the general use of its technology, but, with due cause, has the right to review data located on any storage device, whether on servers or on an individual workstation, with or without prior notification of the user. Suspected inappropriate and/or unlawful use of OSTA computer equipment should be reported to the General Manager immediately.

4. All users who are not employees of OSTA who have access to OSTA technology and electronic files will also be required to sign this agreement, indicating their receipt and understanding of this policy and procedure.

5. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user will immediately exit, attempt to take 'two browser clicks back', and disclose the inadvertent access to management. This

disclosure may serve as a defence against an allegation that the user has intentionally violated OSTA policy and procedure. A user may also, in certain rare instances, access, create, or transmit otherwise unacceptable materials if necessary to complete an assignment, and if done with prior approval and with appropriate guidance from management.

6. Users will exercise extreme caution about revealing personal information to others. For example, passwords should not be shared with family or friends, nor should personal information be divulged.

7. Users will not gain unauthorized access to information resources, another person's materials, information, or files without permission of that person, nor will they attempt to log on as another user.

8. Users will familiarize themselves with and respect copyright laws and licensing agreements. Users will not plagiarize works, for example text or images they find on the Internet, nor will they use another person's property without that person's prior approval or proper citation.

9. Users must keep their expectations moderate. They will not upload or download inappropriately large files, for example music or video files, as determined by the administrator of their account, as network drive space is limited. All uploading, downloading, and printing must occur within the guidelines set by the supervisor/manager.

10. Exclusions – Users will not use OSTA technology:
    a. to conduct or assist to conduct, political campaigns for municipal, provincial, or federal elections, including advocating for or against specific candidates;
    b. to communicate or divulge inappropriate information about individuals;
    c. to conduct a business;
    d. to pursue unauthorized commercial purposes or financial gain unrelated to the business of OSTA;
    e. to offer or provide goods or services, or to advertise products; or
    f. to search for or purchase goods or services for personal use.

11. Users must report any hardware, software or security problem immediately to their supervisor. Unnecessary demonstration of any hardware, software, or security problem to other users is prohibited, as is intentionally finding or exploiting security gaps, experimenting on the network, or using the system in such a way as to disrupt the use of the system by other users.

12. Vandalism is prohibited. Vandalism is defined as any malicious attempt to disrupt, degrade, harm, modify, disable, or destroy data or property of another user or organizations, computer or network hardware or software, wiring or network system itself. This includes, but is not limited to, the uploading, creation, transmission, or installation of computer viruses, viral

files, or malicious software. Use of non-OSTA hardware or software, for example, personal laptops, handheld devices or peripheral devices, on the network environment is prohibited without the authorization of management.

13. The use of any form of electronic communication including email, social media, chats, or newsgroups without an OSTA task/focus/issue constitutes inappropriate behaviour. When using electronic communication, network etiquette conventions apply.

14. The General Manager holds responsibility for the content, management, and maintenance of OSTA's website. The General Manager may, under her/his direction, delegate responsibility for the maintenance of the website.

15. OSTA will attempt to track the source of any inappropriate information, email message, etc., but may not always be able to do so technically, quickly or completely. Therefore users should proceed with caution. OSTA will not be held responsible if a source of trouble cannot be located.

16. Use of any information obtained via the Internet is at the user's own risk.

17. OSTA has web-filtering software. This filtering software helps to block out many objectionable sites, but by no means all of them. If you are aware of objectionable sites, you should report these to management.

18. If an OSTA computer user violates the Use of Computers, Email, and Internet policy or procedure, as stipulated or its intent, one or more of the following consequences may occur:
    a. Suspension or cancellation of use and access privileges;
    b. Payment for damages and repairs;
    c. Discipline under other appropriate OSTA policies or collective agreement, including suspension or termination of employment; or
    d. Civil or criminal liability under other applicable laws.

    Should an infraction occur, OSTA may immediately revoke user privileges at any time. Any user identified as a security risk or as having a history of problems with other computer systems may be denied access to technology.

I have read, had the opportunity to ask questions, understand and agree to abide by **OSTA's Use of Computers, Email, and Internet policy and procedure.**

Date:

_____

_____ _____

Employee's Full Name (Print clearly) Employee Signature