

Chapter 3 Operations Management

3.2 Acceptable Use of Computers, E-Mail and the Internet

Purpose of Policy

The Atlantic Provinces Special Education Authority (APSEA) provides teachers and staff with computer equipment, electronic mail and access to the Internet. As the owner of all computer equipment and e-mail and Internet accounts, APSEA strives to ensure that these technologies are not used in an unprofessional, improper or illegal manner.

Privacy

Because e-mail and Internet communications are being generated for APSEA business on APSEA-owned property, the user should not have any expectation that their e-mail or Internet communications are private.

Staff should be aware that all web access is logged by the server and that these logs may be reviewed by the systems administrators periodically during normal system maintenance.

Statement of Policy

The following policies on the use of APSEA's computer equipment and e-mail and Internet accounts must be strictly adhered to by all users of technologies. Failure to comply with the rules set out below constitutes serious misconduct and will lead to discipline, which could include discharge of access to computer services for personal reasons.

Acceptable Uses

In compliance with these guidelines, employees are encouraged to explore the use of the Internet to further APSEA's goal in a cost-effective manner, to provide service of the highest quality to clients and students and to discover new ways to use these resources to enhance service delivery.

Business Uses:

Employees should use the Internet, when appropriate, to accomplish job responsibilities more effectively.

The Internet provides access to a wide variety of information resources that can aid employees in the performance of their jobs. Examples of job-related use of the Internet are: Accessing external databases and files to obtain reference information, conduct research or develop curricula; corresponding with clients and students; disseminating

documents to individuals or groups; and participating in and reading discussion groups on job-related topics.

Professional Development:

Employees may use the Internet for professional activities and skills development.

The Internet may be used to pursue professional development goals. Examples of professional uses include: Communicating with fellow members of committees in professional organizations; collaborating on studies and articles; connecting to resources that provide information relating to skills development and educational opportunities; and participating in and reading electronic mail discussion groups on professional development topics.

If billable Internet services are encountered by employees during Professional Development activities, employees should check with their supervisor to see if the costs can be recovered.

Personal Use:

At their supervisor's discretion, employees may use the Internet on personal time at work in accordance with the conditions governing access to their work areas. Personal time includes lunch time and the time before and after work. For personal use, billable Internet services are the employee's responsibility and arrangements must be made to reimburse APSEA.

Unacceptable Uses

The following section outlines uses of APSEA's computer equipment and e-mail and Internet systems which are not acceptable and which will result in disciplinary action.

General:

1. All computer equipment and e-mail and Internet systems are to be used solely for work-related purposes or those acceptable uses outlined above. The equipment and e-mail and Internet systems are not to be used for any activity that is illegal or unethical or which could adversely affect the professional reputation of APSEA.
2. Any personal use of the systems and equipment must be of an incidental nature and must not interfere with business activities.
3. All users are required to comply with all federal and provincial laws relating to the use of APSEA's computers and e-mail or Internet systems, as well as APSEA's rules and policies, and any applicable contracts and licenses relating to them.

Abusive, Obscene or Objectionable Uses

4. Employees shall not use abusive or objectionable language in either public or private messages.
5. The e-mail and Internet systems are not to be used to browse, download, transmit or forward obscene, profane, sexually explicit, discriminatory, defamatory, pornographic, threatening or otherwise offensive material, nor to transmit offensive and/or derogatory remarks about a person's race, religion, ethnicity, sex, sexual orientation, age or disability.
6. The e-mail and Internet systems are not to be used to harass, threaten, abuse, embarrass, or cause distress, unwanted attention, or discomfort to any person or entity, by any means.
7. Employees shall not use APSEA's e-mail or Internet systems to post or transmit any message which is libellous, defamatory or which discloses private or personal matters concerning any person.

Illegal Activity

8. Employees may not use APSEA's e-mail and Internet systems to conduct any illegal activity or solicit the performance of any illegal activity or other activity which infringes the rights of others. This includes, but is not limited to: hacking into another computer system; the commission of hate crimes; gambling, and obscenity.

Confidential Information

9. E-mail is not a confidential communications medium and employees should refrain from transmitting sensitive business-related information outside of APSEA over the Internet.
10. Never send strictly confidential messages via the Internet or e-mail.
11. Confidential or sensitive information is not to be transmitted to unauthorized persons or organizations either through the e-mail system or the Internet.

Solicitation/Commercial Uses

12. The Internet, e-mail system and computer equipment are not to be used for personal commercial purposes or financial gain. "Commercial purposes" means offering or providing products or services, or, purchasing products or services. APSEA is not responsible for financial obligations arising from the authorized use of the system for such purposes.

13. Do not enter into contractual commitments using APSEA's e-mail or Internet system.
14. The use of APSEA's e-mail or Internet systems to search for jobs outside of APSEA is expressly prohibited.
15. Staff wishing to use the e-mail system for charitable organization solicitation purposes will seek approval in advance from their Director before doing so. Such request will include the name of the charity, the charity's registration number for income tax purposes, and a draft copy of the proposed e-mail. It is understood that providing such information does not mean that permission will be granted. The decision whether to permit publication by e-mail will rest solely with the Director and must be in keeping with the professionalism of the Atlantic Provinces Special Education Authority.
16. Employees shall not use APSEA's e-mail or Internet systems to post petitions for signatures, chain letters or letters relating to pyramid schemes. Employees shall not post or transmit any advertising, promotional materials or any other solicitation of others for goods or services.
17. Employees shall not use the computers or e-mail and Internet systems for purposes of political lobbying.

Intellectual Property Rights

18. Employees shall respect intellectual property rights at all times when obtaining information over the Internet. Unless the right is explicitly waived, authors of electronic material have copyright and intellectual property rights. Permission must be acquired before duplicating information. Once the author's permission is obtained to use the property, credits must be included.
19. Employees shall not use APSEA's e-mail or Internet systems to post or transmit any message, data, image or program that would violate the property rights of others, including unauthorized copyrighted text, images or programs.
20. Never download or install any commercial software, shareware, or freeware onto network drives or discs without written permission from the Network administrator.
21. Employees shall not use APSEA's e-mail or Internet systems to post or transmit any information that infringes another person's or entity's rights in its trade mark, trade dress, or service mark.
22. Employees shall not use APSEA's e-mail or Internet systems to post or transmit any information that reveals trade secrets belonging to another person, business, service, or other entity.

Netiquette

23. Employees must conform to the specific rules of etiquette or established usage policies for each of the available Internet services. Employees have an obligation to learn about network etiquette (netiquette), customs and courtesies. Accepted procedures and guidelines should be followed when using electronic mail communications, participating in electronic discussion groups, using remote computer services, transferring files from other computers, or disseminating information to others on the Internet.
24. External e-mail communications are to be treated in the same professional manner as with any other written communications from APSEA. Utmost care must be taken in drafting and proofreading the content of external e-mail messages to ensure APSEA's reputation is maintained.
25. Beware of what you say in e-mail messages. Improper statements can give rise to personal or employer liability and may be subject to discipline.
26. Do not use sarcasm or jokes. The absence of nonverbal cues makes this style of communication easy to confuse and may lead to offense. Messages will be treated to mean what is written.
27. Do not send messages that will embarrass you if they become public. E-mail messages, however confidential or damaging, may have to be disclosed in court proceedings or in investigations if relevant to the issues.
28. Employees must not send any correspondence that is not in the best interests of APSEA.

Deceptive/Fraudulent Actions

29. Employees shall not permit non-employees to use APSEA's e-mail and Internet systems.
30. Employees shall not log into APSEA's e-mail and Internet systems under another individual's name.
31. Employees shall not modify files, other data or passwords belonging to other users nor misrepresent other users on any network.
32. Employees will not post or transmit any fraudulent information on or through APSEA's e-mail and Internet systems. This means any information that you know or have reason to know is false, and that you intend for others to rely on.

Invasion of the Privacy Rights of Others

33. Although the use of APSEA's computers, e-mail and Internet systems are subject to monitoring by APSEA, employees are expected to respect other users, and to not enter, monitor, or otherwise interfere in their use of company computers or electronic communications, or to use company computers to enter, monitor or otherwise interfere with third parties.

Destructive Uses

34. Employees shall not use the network in such manner as to disrupt the use of the network by others. Hardware or software shall not be destroyed, modified or abused in any way.
35. Employees shall not post or transmit any file which contains viruses, worms, "Trojan horses" or any other contaminating or destructive features.
36. Employees must not abuse the system by causing harm to the system or inhibiting other users' ability to effectively use the system. This includes, but is not limited to:
 - (a) The importation into the system of a virus or other harmful programming. Never import files or unknown messages onto your system without having them scanned for viruses.
 - (b) Users are expected to remain within allocated disk space and delete e-mail or other materials which take up excessive storage space:
 - (c) Do not create e-mail congestion by sending trivial messages or unnecessarily copying e-mails and do not advertise by e-mail or send messages for missing items unless urgent for business reasons.
 - (d) Chain letters and "spamming" are expressly prohibited. "Spamming" is sending an annoying or unnecessary message to a large number of people (20 or more).

POLICY ENFORCEMENT

All computer equipment and e-mail and Internet systems are the sole property of APSEA. As such, APSEA reserves the right to monitor the use of these technologies to ensure they are being used in a proper, ethical and legal manner. Daily Internet and e-mail activity may be audited to ensure compliance.

These systems, including the equipment and the data stored in the system, are and remain at all times the property of APSEA. As such, all messages, created, sent, received, or stored in the system are and remain the property of APSEA. APSEA reserves the right to retrieve and review any messages composed, sent or received. Please note that even when a message is deleted or

erased, it is still possible to recreate the message: therefore, ultimate privacy of messages cannot be ensured to anyone.

As the sole owner of all data stored on individual hard drives and the network, APSEA reserves the right to take whatever steps are necessary at any time to gain access to such information.

All information stored on individual hard drives and the network is the sole property of APSEA. Removal of such information upon departure from APSEA is prohibited. Users are not permitted to password protect information stored on the individual hard drives or the network unless requested to do so by APSEA. All passwords must be made known to APSEA as your system may need to be accessed by APSEA when you are absent.

Failure to use APSEA's computer equipment and e-mail and Internet systems in accordance with the policies set out herein could result in discipline and/or termination where appropriate. Anyone who may be aware of or receives discriminatory, offensive, sexually explicit or otherwise inappropriate material is encouraged to immediately report such incidents to their Director so that measures can be taken to avoid improper use of electronic communications network.

Authority: Board Minute
Date of Adoption: December 13, 2000