Acceptable Use of Technology for Employees
Administrative Procedure

Department: Human Resources
Section: Employee and Labour Relations

Employees of the Annapolis Valley Regional School Board are responsible for the acceptable use of information technology.

Specifically

1.0 Information technology is defined as any computer-based tool that people use to work with information, and support the information and information-processing needs of an organization. (*Management Information Systems for the Information Age*, 2001)

2.0 Computer hardware and software provided to employees is the property of the Annapolis Valley Regional School Board.

3.0 Employees will not install any unapproved software on Board computers, such as Kazaa, ICQ, etc. Any unapproved software may be removed without consent of the user. Unauthorized software includes any software that is unlicensed.

4.0 Employees will not download or transfer pirated software to or from computers.

5.0 Employees will not use the Board system and network to violate copyright laws or usage licensing agreements and will not plagiarize work from the Internet.

6.0 Employees shall not access, review, upload, download, store, print, post or distribute pornographic, obscene or sexually explicit material or materials that use language or images that promote/advocate violence, harassment or discrimination (hate literature).

7.0 Employees will not use the Board network to gain unauthorized access to information resources.

8.0 Employees will not attempt to gain unauthorized access to any network, including the Board's.

9.0 Employees will not attempt to connect unauthorized hardware (including personal laptops) to the Board's network without the permission of Board technology staff in consultation with the school principal/site manager.

10.0 Employees will not use the Board network for unauthorized commercial purposes, including product advertising and the sale of goods and/or products.

11.0 Access to the internet by employees, including the web and e-mail, is intended to support job related duties and responsibilities.

12.0 Personal use by employees is expected to be kept at a minimum.

13.0 Employees are not permitted to play network-based games, including on-line gambling.

14.0 Any excessive use for personal reasons during the work hours will result in disciplinary action.

15.0 Employees will not knowingly jeopardize the integrity of the Board system and networks.

16.0 Employees will not use the Board network to post personal information on the Internet, such as the set-up and maintenance of personal web pages.

17.0 Employees will not disrupt or congest network and/or systems, for example by "streaming" music, movie trailers, flooding the network with messages or sending chain letters or pyramid salutations.

18.0 Employees should be aware that e-mail messages may be monitored from time-to-time as part of regular maintenance/security checks.

19.0 Employees will not disclose private communications without permission to parties other than the intended recipient, or disclose confidential or private information.

20.0 Employees will not conceal their identity or impersonate another person when posting or transmitting messages.

21.0 Employees will not post or transmit any information or software that the employee knows contains a virus, worm or other harmful component.

22.0 Employees will not share their internet dial-up account outside of their immediate household, including permitting third parties to use the Board's internet access account and password.

23.0 Employees will not use information technology facilities to interfere with the operation of Board information technology systems and connecting networks.

24.0 Remote access by employees will be strictly controlled with one-time password authentication.

25.0 Employees must have approval from their immediate supervisor and the Coordinator of Management Information Systems to use remote access.

26.0 Remote access connections are literal extensions of the Board's network and provide a potential path to confidential and private information. Employees with remote access privileges must make every reasonable effort to protect the Board's information technology system.

27.0 Employees with remote access privileges:

27.1 Will ensure that a connection to the Board network is not accessed by non-authorized users.

27.2 Will sign a Remote Access Procedure Agreement (attached as Appendix A).

27.3 Will be aware of responsibilities under the *Freedom of Information and Protection of Privacy Act (Nova Scotia)*.

27.4 Will ensure that all applicable Security Patches are immediately installed on any computer used for remote access purposes.

27.5 Must use up-to-date anti-virus software on any computer being used for remote access.

27.6 Must ensure that no master data is saved on a computer that is not owned by the Board.

28.0 Employees will not engage in the use of chat lines or variants of Internet Relay Chat (IRC) without approval of the network administrator in consultation with the school principal/site manager.

29.0 Any perceived or actual violation of the Acceptable Use Policy is to be reported to the employee's immediate supervisor. The immediate supervisor is responsible for advising the Coordinator of Management Information Systems. If it is determined that the employee has violated the Acceptable Use Policy and Administrative Procedure, then the immediate supervisor shall be responsible for initiating disciplinary action, in

accordance with the provisions of the appropriate collective agreement or terms and conditions of employment.

Monitoring

- The Director of Human Resources is responsible for the implementation, monitoring and revision of this administrative procedure.
- This administrative procedure will be monitored annually.

Superintendent Approved: July 4/05
Ref: BP 305.20
Monitoring Date: Annually
Revised: