Department: Human Resources
Section: Employee and Labour Relations

Employees of the Annapolis Valley Regional School Board must adhere to this policy and its procedures. Proper implementation of this policy will achieve the following objectives:

- ensure employees have the information they need to demonstrate good digital citizenship, sensitivity, and respect through appropriate and responsible behaviour when using technology;
- clarify expectations and responsibilities related to use of technology; and,
- ensure an awareness of Board policy and legislation.

Technology Management

1.0 Technology is defined as any digital tool that people use to work with information, and support the information and information-processing needs of an organization.

2.0 Any technology provided to employees is the property of the Annapolis Valley Regional School Board.

3.0 Employees should be aware that Board technology will be monitored from time to time as part of regular maintenance and security.

4.0 Employees must have approval from their immediate supervisor and the Coordinator of Information Technology to use remote access, including standard user access. Employees may need to complete appropriate documentation for security access.

5.0 Employees with remote access privileges:

- 5.1 will ensure that a connection to the Board network is not accessed by non-authorized users.
- 5.2 will use strong password security, including but not limited to, avoiding the use of auto-saving passwords.
- 5.3 will ensure that appropriate security measures are maintained on any computers used.
- 5.4 must ensure that no sensitive and/or confidential information is saved on a computer that is not owned by the Board.

Acceptable Use of Technology

6.0 Access to technology by employees is intended to support job-related duties and responsibilities. Use technology for authorized purposes only. Personal use by employees is expected to be kept to a minimum.

7.0 Elevated 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.

8.0 Use technology in a responsible and ethical manner consistent with the purposes for which it is provided.

9.0 Maintain appropriate online behaviour.

10.0 Exercise caution when releasing one's own or another person's personal information online.

11.0 Respect their own and others' intellectual property.

12.0 Install and access only authorized software and hardware on Board-provided devices.

13.0 Report suspected vandalism, unauthorized file access, or inappropriate use of technology to one's supervisor.

Unacceptable Use of Technology

14.0 Employees will not install any digital tool that contravenes existing policies and licensing or violates copyright laws.

15.0 Employees shall not access, create, solicit, communicate, or distribute harassing, pornographic, obscene, racist, sexually explicit, or threatening material, imagery, or language.

16.0 Employees will not use Board technology to gain unauthorized access to information. Employees will not attempt to gain unauthorized access to any Board technology resource.

17.0 Employees will not use Board technology for unauthorized commercial purposes, including product advertising and the sale of services or goods.

18.0 Employees will not knowingly jeopardize the integrity of Board technology.

19.0 Employees will not use Board technology for unprofessional conduct. Unprofessional conduct includes but is not limited to:

- 19.1 attempting to access or make public, the private or personal materials, information, or files of others without appropriate consent.
- 19.2 using technology for the purposes of cyberbullying.
- 19.3 causing disruption of technology databases or systems.
- 19.4 vandalizing, damaging, or disabling the work of others.
- 19.5 accessing, manipulating, altering, or attempting to damage, disable, or destroy technology or files belonging to others.
- 19.6 any use that violates provincial laws, federal laws or other AVRSB policies.

Consequences of Unacceptable Use of Technology

20.0 Any perceived or actual violation of the Acceptable Use of Technology for Employees Policy is to be reported to the employee's immediate supervisor. The immediate supervisor is responsible for advising the Coordinator of Information Technology. If it is determined that the employee has violated the Acceptable Use of Technology for Employees 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.

21.0 Unacceptable use of technology by a Board employee shall be determined through the Board's disciplinary investigation and response processes resulting in appropriate disciplinary measures up to and including termination. Where appropriate, this may include loss of access to technology and/or referral or involvement of law enforcement.

22.0 Unacceptable use of technology by a volunteer will be addressed by the principal and may include conditions to suspension of or termination of volunteering, loss of access to technology and/or referral or involvement of law enforcement.

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: October 13/17