AVON MAITLAND DISTRICT SCHOOL BOARD
ADMINISTRATIVE PROCEDURE
NO. 140

SUBJECT: TECHNOLOGY: RESPONSIBLE USE AND SECURITY

Legal References: *Education Act: Section 265 Duties of Principal: Care of Pupils and Property; Part Xiii— Behaviour, Discipline and Safety Ontario Regulation 298—Operation of Schools Section 20 Duties of Teachers—Safety Procedures; Section 23 Requirements for Pupils Guideline—Ontario Schools Code of Conduct; Criminal Code of Canada; Canadian Charter of Rights and Freedoms; Ontario Human Rights Code; Municipal Freedom of information and Protection of Privacy Act*

Related References: *Administrative Procedure 112 Communications and Media Relations; AP 138 Positive Workplace Environment; AP 190 Copyright; AP 194 Privacy and Breach Protocol; AP 320 Use of internet and Electronic Devices by Students; AP 351 Code of Conduct; AP 352 Promoting Positive Student Behaviour; AP 353 Student Suspension; AP 354 Student Expulsion; AP 356 Substance Abuse by Students; AP 357 Violence-Free Schools; AP 400 Recruitment, Hiring and Selection of Staff; AP 404 Violence Prevention in the Workplace; AP 405 Allegations Against Employees and Volunteers; AP 440 Employee Conflicts of interest; AP 516 Purchasing Procedures; Guidelines for Email Management; Guidelines for Google Drive; Guidelines for Encrypting*

1. Expectations for Technology Use

1.1 The Director of Education has established expectations with respect to technology and information resources, security procedures, and the roles and responsibilities of each individual in maintaining a secure computing environment.

1.2 Since students and staff members have access to computer and Internet resources as part of their teaching/learning/work experience, they each have a role in maintaining a secure computing environment. As well, trustees, school council representatives, and partners and/or volunteers with approved access to technology at the school have the same responsibility for acceptable use and security in the computing environment.

1.3 Principals and management personnel are responsible for communicating expectations and ensuring compliance with safe computing practices. This includes the annual distribution of the following:

- Appendix B - Student Code of Conduct
- Form 140A - Letter to Employees
- Form 140B - Letter to Students and Parents/Guardians
- Form 103C - Found in Maplewood - Confirmation of Emergency Contact and Personal Information Form

2. Principles of the Use of Digital Resources

2.1 Information technology equipment and data owned by the board are to be used solely to further the board's objectives and to be consistent with the law, the *Canadian Charter of Rights and Freedoms* and the *Ontario Human Rights Code.* Employees should not use Board-owned equipment for the creation or storage of personal information that they expect to remain private and confidential.

2.2 The Director recognizes and respects all disclosure and privacy protection obligations as required by the *Municipal Freedom of information and Protection of Privacy Act.*

2.3 Avon Maitland District School Board's information is a corporate resource with substantial value that must be protected from unauthorized modification, destruction or disclosure, whether intentional or inadvertent.

3. Secure and Protected Computing Resources

3.1 The Board has delegated responsibility to the Director of Education for securing its computing systems against unauthorized access and/or abuse while making them accessible for authorized and legitimate uses.

3.2 It is important for all users of Board-owned equipment to practice responsible and ethical behavior in their computing activities. Many staff members have access to private and sensitive information that could injure other persons and/or diminish the reputation of the Board if lost or disclosed inadvertently.

3.3 With increasing dependence on electronic information systems for all aspects of day-to-day operations, it is essential that computing resources and information are secure and protected from disruption.

3.4 In order to protect the integrity of information stored on computers in schools and administration facilities, it is essential that responsible security practices are followed.

3.5 Individuals and the corporation may be held liable in the event that software is not licensed or properly authorized or if information is not properly and securely stored.

4. Implementation Procedures

4.1 Everyone has a part in maintaining a secure computing environment and must adhere to the procedures outlined in this document.

4.2 Practices have been identified to promote proper password management, Internet access and responsible use of shared resources.

4.3 All technology users approved by the Director or designate(s) are asked to read this document carefully.

4.4 Anyone with questions regarding this procedure should submit an eBase work order for follow-up by the Administrator of Information Technology.

5. Definitions

5.1 Appendix A presents definitions of technical terms used in this document.

6. Directions for Access and Use

6.1 Access to confidential information is restricted to those with a demonstrated "need to know" to the extent required to perform job functions.

6.2 Access to confidential electronic information will be granted only to appropriate individuals and work groups, as described below in Section 7.

6.3 Critical data are securely managed throughout the life cycle and backed up on a regularly scheduled cycle.

6.4 Information retention and equipment disposal practices ensure the continued protection of personal and corporate privacy.

6.5 All digital technology and software purchased by the Board, belong to the Board and the Board reserves the right to access, monitor and review all use, including email and Internet use, and file contents at any time.

6.6 The Board reserves the right to review, access, monitor, delete or otherwise deal with any material stored on the Board's system without further notice.

6.7 Software and related intellectual property developed by staff members in the performance of their duties are the property of the district, and may not be distributed or shared unless authorized in writing by the Director of Education or designate (see Administrative Procedure 440 Employee Conflicts of Interest).

6.8 All software residing on AMDSB technology must be installed in compliance with licensing requirements of the software's owners. Use of "pirated" software or software secured through unauthorized reproduction is strictly prohibited.

6.9 Passwords and related security codes must be kept secure at all times and disclosed only as provided for by the disclosure policies and practices of its owners.

7. Responsibilities of Staff Members

7.1 Primary responsibility for security of information is vested with the supervisory officer designated by the Director to be responsible for the creation or assembly of the information (e.g., security of human resources records is vested with the Superintendent of Education (Human Resources)). A supervisory officer may delegate this responsibility to a principal or other senior staff member and these individuals may delegate this responsibility to other staff members, providing that such delegation is in writing.

7.2 Supervisory officers, principals and managers are accountable for ensuring that staff members are informed of this procedure and that compliance occurs.

7.3 New staff members will receive an information letter (Form 140A), together with a copy of this administrative procedure, as part of the hiring orientation. Attention should be drawn to the section regarding Internet access.

7.4 Secondary responsibility for the security of information is vested with the Information Technology department staff who manage information processing, transmission, and storage in compliance with the district's Records and Information Management Program and in consultation with the Enrolment and Information Manager.

7.5 Users of information are responsible for using it for the purposes intended and complying with control, access and disclosure procedures.

7.6 Individual users are responsible for the information which is in their possession (downloaded onto their computer or portable data storage device).

7.7 Those responsible for its use and physical security must protect data, digital technology and software at all times from physical damage, theft or unauthorized modification.

7.8 Computers or terminals must not be left unattended when the power is on and confidential or critical information is being accessed. Users must log-off their computers when the computer is to be left unattended for a prolonged period of time. Users must log-off at the end of each work day.

7.9 Where confidential or sensitive information is stored on a computer's hard drive, every effort must be taken to ensure that the computer is physically secure, information is backed up, and sensitive materials are protected by logical access controls such as passwords.

7.10 The board's "employee exit" procedure for all staff members must include review with the current supervisor and removal or reassignment of any electronic files created by the departing individual on the server and/or hard drive. Likewise, any data on that staff member's home computer, which would be considered the property of Avon Maitland District School Board, must also be removed by the departing staff member. This includes the removal of board software from home computers, if applicable. A staff member sign-off form for this purpose will be included in the "employee exit" procedure maintained by the human resources department.

7.11 Staff must follow the procedures outlined in AP 103 Management of Personal Information - Student

7.11.1 Specifically, staff must ensure that:

7.11.1.1 Laptops, iPads, cell phones and electronic storage media are password protected to prevent unauthorized access;

7.11.1.2 Devices containing confidential information are kept under direct supervision of the staff member or stored in a secure, locked location when outside of the worksite;

7.11.1.3 Devices containing confidential information are not shared with individuals who do not have the rights or responsibilities to view the information contained on such devices (for example, family or friends); and

7.11.1.4 When using wireless devices confidential information is not transmitted over unsecured networks.

7.11.2 Failure to comply with this Administrative Procedure 140 Technology: Responsible Use and Security will result in disciplinary action that may include dismissal.

8. Computer Security Practices

8.1 Computer Viruses and Related Problems

8.1.1 Computer viruses and related problems can cause extensive damage to computer systems. There are thousands of computer viruses currently in existence with new ones appearing frequently. Viruses can be spread by a variety of means— downloading files from the Internet, bulletin boards, shared drives, infected media (e.g., flash drives, downloaded files) and email attachments.

8.1.2 Vigilance is necessary to protect against infection and proliferation of viruses and related problems. Computer users can reduce the chances of infection and damage in several ways:

8.1.3 Updating software regularly is necessary to obtain protection against the most recent viruses;

8.1.3.1 Use antivirus software to scan all files downloaded or copied to personal computers;

8.1.3.2 Obtain software from reputable sources;

8.1.3.3 Do not open any e-mail messages or email attachments that appear suspicious;

8.1.3.4 To help email recipients distinguish genuine email from virus infected mail, give meaningful descriptions in the subject area and, when sending an attachment, indicate in the body of the message what the attachment contains and what program was used to create the document (e.g., *Word, Excel);* and

8.1.3.5 Back up important files regularly to minimize data loss should your system become infected with a virus.

8.1.4 Common symptoms of virus infection include unusual messages or displays on the screen, missing and inaccessible or unusable files or programs.

8.1.5 Staff members are asked to submit an eBase IT Work Order in the case of a suspected virus.

8.1.6 The creation and distribution of virus hoaxes can result in wasted resources (staff time to investigate and correct any actions taken in response to hoaxes, and increases in email traffic). Individuals who receive virus alerts from persons or organizations outside the District are asked to forward the information to the IT Department through an eBase Work Order.

8.2 Software and Licenses

8.2.1 Individuals and the district may be held liable if software is not licensed or properly authorized or if information is not properly and securely stored.

8.2.2 Software License agreements must be honoured even if the software is not copy- protected. All software used for district operations must be installed in accordance with licensing agreements.

8.2.3 Original license agreements purchased under the Information Technology department budget are filed centrally.

8.2.4 Any software purchased at the school level must have appropriate site or individual licenses stored at the school by the principal or designate

(Technical Resource Assistant or Site Contact). Note: Tech Team members will ask to see licenses prior to any installation being completed.

8.2.5 *Microsoft Office* is the standard administrative package used for business practices within the central administrative office, satellite locations and all school offices.

8.2.6 Software purchased for home use is not licensed for use on Board-owned equipment and therefore may not be installed on Board computers.

8.2.7 It is against the law to copy commercial software that has not been placed in the public domain or distributed as "freeware." Software "piracy" (copying a commercial software product purchased by a party other than the user) injures everyone. It reduces the incentives for the software industry to invest in new projects, reduces the willingness of vendors to support board computing through discount programs, and makes violators vulnerable to criminal prosecution. Users are not permitted to remove software from the Board system for use on other systems as this may amount to copyright infringement and expose both the individual and the Board to liability.

8.3 Digital Technology Hardware

8.3.1 Computer equipment (including monitors, system units, printers, keyboards, external disk drives, scanners, key pads, mouse, cables, etc.) must be located where they will be secure and as free as reasonably possible from damage by water, fire, or other disasters.

8.3.2 Laptop computers, iPads and other related mobile equipment must be handled securely, as the high value and portability of these devices makes them desirable theft items.

8.3.3 Personal computer equipment (laptops, personal data devices, etc.) may not be directly connected (hard-wired) to the Board's LAN or WAN for security reasons. However, personal computer equipment may be connected to the Board's wireless network Staff and students must ensure that their computer/device meets the following conditions:

8.3.3.1 the device must have an up-to-date antivirus program running;

8.3.3.2 operating system security patches must be up to date;

8.3.3.3 p2p programs (such as Frostwire) must not be running; and

8.3.3.4 there must be no viruses, worms, malware, etc. on the device.

8.3.4 If any of these conditions are not met, the Network Authentication Control will deny access to the wireless network.

8.4 Digital Technology Purchases

8.4.1 Any technology purchases must follow the procedures outlined in AP 516 and the IT purchasing tri-angle.

8.5 Removable Media

8.5.1 Data may be stored on removable media such as external hard drives.

8.5.2 Important data must be appropriately backed up.

8.5.3 When not in use, removable media must be placed in locked storage if the data contained are critical or confidential. Loss of data can occur if removable disks are stored near magnetic fields (telephones or monitors).

8.5.4 Instructions for safe and proper use provided with removable media must be followed. As with other computer equipment, foreign objects such as food, liquids and dust can cause damage to removable media. Excessive heat and direct sunlight may also cause damage to such media. Valuable data can be lost if media are not handled safely.

8.5.5 Students and staff may use Portable Storage Devices for the storage and transfer of documents between school and home, however the use of Google Drive for this purpose is recommended. The protocol for use of such devices by students is outlined in Appendix B: Technology Responsible Use and Security - code of conduct for Students.

8.6 Documentation

8.6.1 Individual users are responsible for the care and usage of software manuals and reference manuals for hardware and related equipment. It is each person's responsibility to take reasonable precautions so that these are not lost, stolen, or damaged.

8.6.2 Printouts that contain confidential information must be stored securely.

8.7 Contingency Plans/Backup

8.7.1 In cases of emergency, an eBase IT Work Order should be submitted by the school Technical Resource Assistant or Site Contact or a phone call should be made to the Information Technology Department. The Administrator of Information Technology will be notified immediately.

8.7.2 Every department, in consultation with the Information Technology Department, must have contingency plans in place to deal with hardware and software failures or other related emergencies.

8.7.3 To protect critical information from loss in the event of theft or fire, all systems are to be backed up on a regular basis. Backup copies are to be stored in a secure, fireproof location other than that of the computer workstation. A regular routine to perform backups for servers and personal computer data must be established.

8.7.4 Where confidential or sensitive files are stored on a hard disk, precautions must be taken to ensure the files are appropriately protected from inadvertent or deliberate loss or tampering. These files must be copied (backed up) periodically.

8.8 Password/User Authorization

8.8.1 Board employees must each have a unique login and password for access to Board technology, including Active Directory, Maplewood, GAFE, and all services located within the Education Centre.

8.8.2 Passwords of Board employees are not to be posted in public access areas or near the computer itself. Individual user passwords must remain secure and must not be shared with anyone else.

8.8.3 The following requirements will be in place for password protection:

8.8.3.1 passwords must be a minimum of eight characters in length.;

8.8.3.2 passwords must contain an uppercase character, a lowercase character, and a number;
8.8.3.3 passwords must be changed every 90 days;
8.8.3.4 when prompted to change their passwords, users may not re-use any of the eight most recently used passwords;
8.8.3.5 users will be locked out after six failed attempts to log in;
8.8.3.6 the lockout will be for a minimum of 30 minutes or until a system administrator has re-enabled the user ID; and,
8.8.3.7 users will have to re-authenticate to the system after 15 minutes of inactivity.

8.9 Data Integrity

8.9.1 The input of **sensitive** or **critical** information must be accurate and complete and must be subject to error checking.

8.10 Electronic Mail, Conferencing & other On-line Communications

8.10.1 Board administrative staff will determine Internet programs, users, and protocols etc. for standardization within Avon Maitland District School Board.

8.10.2 The Director of education may designate individuals to monitor or check from time to time the contents of electronic messages carried on district computer networks. All communications, including those marked as private/confidential by the sender, may be monitored. Electronic mail originating from the district, like traditional mail, is to be used only to further the district's objectives, and is the property of Avon Maitland District School Board. All communications are to use appropriate and respectful language while adhering to the law, the Canadian Charter of Rights and Freedoms and the Ontario Human Rights Code.

8.10.3 Email communication for key Board personnel will be archived for up to two years from the date of the original communication.

8.10.4 For further clarification, review the Email Protocols document, attached Appendix C. The provisions outlined in AP 140 Technology: Responsible Use and Security as well as in AMDSB Administrative Guideline No. 11: Guideline for Email Management and in AMDSB Administrative Guideline No. 12: Encrypting Data Files apply when using Board email both during and outside regular working hours.

8.11 Internet Access

8.11.1 The Director of education or designate(s) provides connections to the Internet for staff and student use that is consistent with district objectives. Use of the district's Internet access for purposes other than the furtherance of the objectives of Avon Maitland District School Board may result in disciplinary action.

8.12 Online Publishing

8.12.1 All web pages hosted on the board's corporate site or provided for by the board are considered the property of the Avon Maitland District School Board and must comply with the principles and standards set out in this procedure. Online publishing must respect the administrative procedures and be consistent with copyright and other laws, the *Charter of Rights and Freedoms* and the *Ontario Human Rights Code* and the *Municipal Freedom of Information and Protection of Privacy Act.*

8.13 Public Cloud Computing

8.13.1 There are cloud based services that provide an opportunity for communication and collaboration between teachers and parents. Many staff may wish to use these tools to increase parent engagement. Systems like D2L Parent Portal, Compass for Success Parent Portal, and Google Classroom Guardian have security and privacy agreements in place.

8.13.2 The Board's Privacy and Security requirements must be met before staff use collaboration services to communicate with parents. Therefore, staff must follow the process outlined below before any invitation is sent to parents to participate in communication/collaboration services.

8.13.3 Determine which parent/guardian email will be used within the collaboration tool. This review may include custody and/or contact parameters outlined within custodial agreements. Please note: the approved parent/guardian email address(s) are visible within the parent/guardian information section of Maplewood ConnectEd.

8.13.4 Students 18 years of age or older must provide written consent at the school level before parental access is granted.
Teachers are reminded that public cloud tools should not be used for posting student marks or school work.

9. Technology Responsible Use Practices for All Approved User

9.1 Digital technology users approved by the Director or designate(s) with access to computers at the schools and administrative offices include students, employees, trustees, school council representatives, and partners/volunteers with approved access.

9.2 All approved digital technology users are required to use technology and the district's information resources in accordance with this administrative procedure.

9.3 The use of board-owned technology, network and licensed software as well as access to the Internet using board equipment must be in support of education and educational research, and be consistent with the educational objectives of Avon Maitland District School Board.

9.4 Unacceptable or inappropriate use includes, but is not limited to:

9.1.1. Activities which may damage equipment;

9.1.2. Downloading, copying, viewing or transmitting any material which is in violation of any federal or provincial statute or regulation such as copyrighted material; threatening or obscene material; hateful, racist or discriminatory material;

9.1.3. Any breach of security on local and remote sites including use or attempted use of another user's account; unlawful entry or attempted entry into any network system; any attempt to gain unauthorized access to view, alter, copy, share or destroy data and the creation and/or willful transmission of computer viruses or virus hoaxes; and

9.1.4. Activities supporting private business or commercial ventures except in the appropriate conference designated by the Information Technology Department.

9.1.5. Creation or using a VPN (Virtual Private Network) or Proxy Server other than the Boards authorized VPN system.

9.1.6. Any breach in privacy occurring on any technology within the Avon Maitland District School Board must follow our procedure outlined within AP 194 Privacy and Breach Protocol.

10. Reserved Right to Limit Use

10.1 The Board, in its sole discretion, has the right to limit individual or organizational use at any time without notice.

10.2 Network etiquette must be followed, including using appropriate and respectful language, the avoidance of the distribution of nuisance or junk mail and the efficient use of on-line time.

10.3 Students must follow personal safety measures including, but not limited to, the following:
- 10.3.1 Report to school staff any unusual or suspicious communication with others;
- 10.3.2 Do not divulge any personally identifying information over the Internet; and
- 10.3.3 Never agree to meet with strangers with whom they have communicated on the Internet.

10.4 Use of the Internet is an integral part of the educational experience in many school programs and schools must inform parents that their child will use the Internet. Form 140B contains information for parents regarding computer and Internet usage. Form 103C Confirmation of Emergency Contact and Personal Information Form, which is a parent/guardian acknowledgement for the student's use of technology will be issued by the school annually.

10.5 Adult students will be informed about expectations for their use of computers and the Internet (Form 140B). Form 103C Confirmation of Emergency Contact and Personal Information Form, which is an adult student specific acknowledgement for the student's use of the technology will be issued by the school annually, or, in the case of Adult Learning Centres, at the time of registration.

10.6 Inappropriate use of the district's digital technology resources will result in consequences. In the event of actions, which may violate the law, the police will be informed.

11. Canada's Anti-Spam Legislation (CASL)

11.1 Canada's Anti-Spam Legislation (CASL) prohibits the sending of a commercial electronic message (CEM) to an electronic address unless the sender complies with 3 requirements
- 11.1.1 obtains the consent of the intended recipient;
- 11.1.2 provides certain identification information of the sender; and
- 11.1.3 provides an unsubscribe mechanism.

11.2 Anyone who is unsure as to whether or not an electronic message being sent to an electronic address is a CEM should consult with the Administrator of Information Services prior to sending any such message.

11.3 No one is permitted to use their Board issued email address to promote or advertise participation in non-Board or personal commercial activities, including fundraising awareness to individual GAFE mailboxes or an individual's external email address.

11.4 Schools often communicate with parents and students by emailing newsletters or other forms of communication. If these electronic communications include encouraging participation in a commercial activity as described in the definition section above, then written consent of the recipient must be obtained prior to sending such a message. This written consent is captured on the Student Registration Form and tracked within the Maplewood student record. Principals are responsible to ensure all electronic mailing lists used by the school office staff or teaching staff contain only the email addresses for which CASL consent has been received. During a three-year transition period (to July 1, 2017) consent is implied for parties who are in an existing relationship. After July 1, 2017 schools must have written consent.

12. Unsubscribe Mechanism

12.1 A CEM must also include an unsubscribe mechanism through which a recipient of a CEM may indicate that they no longer wish to receive such messages.

12.2 The sender must specify in the CEM that the recipient may unsubscribe to future CEMs by replying to the CEM and indicating "unsubscribe" in the subject line. The following statement must be included within the footer of each CEM.

12.3 This message is being sent on behalf of the Avon Maitland District School Board and/or your child's school in compliance with the Canadian Anti-Spam Legislation. Questions regarding this electronic communication may be referred to the Principal of the school or the Enrolment and Information Manager at the Education Centre.

12.4 You may unsubscribe from receiving these messages by REPLYING to this email with "unsubscribe" in the subject line.

12.5 Any requests to unsubscribe must be acted upon no later than 10 business days from receipt of it. The email address must be removed from the mailing list.

12.6 For schools, the Maplewood record should be updated and the printed copy of the unsubscribe email should be placed in the documentation folder of the OSR with the original student registration form. For example, if a school sends newsletters electronically to parents and/or students and the newsletter contains from time to time promotions or advertisements to sell products or services including for fundraising events, and a parent or student has indicated they do not wish to receive CEMs, then the person's electronic address will be removed and the newsletter or other communication will be sent home with the student.

12.7 School Principals should strive to ensure that only one person is responsible for maintaining a list of electronic addresses to which CEMs are sent and that person must be notified of any unsubscribe requests or revocation of consent.

12.8 All departments of the Board should follow procedures for maintaining electronic addresses for the purposes of commercial electronic messages and deleting those addresses that request to unsubscribe. Consultation with the Enrolment and Information Manager may be required. An "opt out" option must be included within the email and the following statement must be included in the body of commercial electronic messages.

12.9 This message is being sent on behalf of the Avon Maitland District School Board in compliance with the Canadian Anti-Spam Legislation. Questions regarding this electronic communication may be referred to the sender of this email or the Enrolment and Information Manager at the Education Centre.

12.10 You may unsubscribe from receiving these messages by REPLYING to this email with "unsubscribe" in the subject line.

13. Digital Citizenship

13.1. Today's world is vastly different than the world was a decade ago, a year ago and even a month ago. The explosion of technology has vastly changed the way students learn as well as our view of community and what it means to be part of and interact within that community. As such, while the base qualities of being a good citizen haven't changed, the notion of citizenship must now encompass the idea of being a good digital citizen. Today's students need to have the skills to actively participate in the complexities of digital spaces in a positive, responsible and safe manner. The Avon Maitland District School Board is currently developing a Digital Citizenship AP and Handbook to support staff, students and parents to become good digital citizens who have the skills to be successful in both the world we live in today and the rapidly changing world of the future.

14. Acknowledgement

14.1 Permission was received from Thames Valley District School Board to use its ***Board Computer Security*** procedure as a guideline in developing this Avon Maitland District School Board administrative procedure.

Appendix A: DEFINITIONS

For the purpose of this document the following definitions will apply:

Access

- To approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of digital technology or computer network.

Board's Information Resources

Hardware:	CPUs, computer boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers, iPads, Chromebooks
Software:	source programs, object programs, utilities, diagnostic programs, operating systems, communication programs
Data:	during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media Documentation: on programs, hardware, systems, local administrative/academic procedures
Supplies:	paper, forms, ribbons, magnetic media

Canada's Anti-Spam Legislation (CASL)

- Commercial Activity: Includes any particular transaction or conduct that is of a commercial nature. This includes an offer to purchase, sell, barter, or lease products, goods, services or land and an advertisement or promotion of any of those activities. Examples include the promotion, advertising and/or offering for sale of school pictures, field trips, yearbooks, team uniforms, products or services for fundraising events, requests for proposals, invitations to bid, offering of courses locally or abroad for a fee, etc.
- Commercial Electronic Message (CEM): CEMs are an electronic message sent to an electronic address, where it is reasonable to conclude that the message's purpose or one of its purposes is to encourage participation in a commercial activity.
- Electronic Message: means a message sent by telecommunication including email, texting, other instant messaging, etc.
- Electronic Address: an address used in connection with the transmission of an electronic message to an email, instant messaging account, telephone account, Facebook, or any similar account. Faxes, voicemails, and interactive two-way voice communications between individuals are excluded from the definition of electronic address.

Computer Network

- A number of computers connected together that are capable of sharing common resources such as files and printers

Computer Program

- A set of instructions that tells the computer what to do

Computer Software

- Programmed instructions whether purchased or written by the user that the computer carries out

Confidential / Sensitive Information

- Information which requires protection from unauthorized access and is regulated by a legislation or policy: for example; personally identifiable student data such as grades and test results

Contingency Plans

- Are alternative steps to take when information technology support is interrupted. Contingency plans assure that you can continue to perform essential functions in the event that you lose access to data and equipment resulting from a number of reasons (theft, equipment failure, fire/water damage, unauthorized access, etc.)

Critical

- Critical information, networks, applications, systems, or data, are those resources determined by the Director to be essential to the district's critical functions

Digital Citizenship

- The safe, responsible and ethical use of technology by students and staff following accepted norms and rules to support collaboration and learning and the development of a positive digital footprint

E-mail

- "GAFE" Google Apps for Education the district's electronic mail system

Freeware

- Software that is available for free use

Intellectual Property

- Data, including programs, which are subject to copyright protection as "personal" property or "board" property.

Internet

- A logical network of tens of thousands of interconnected host computers

Performance of their Duties

- Relates to job duties as specified in the staff member's job description

Property

- Anything of value, includes but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value

Shareware

- Software that is available for free evaluation. Generally, you are obligated to pay a license fee in order to use it on a continuing basis

Software License

- An agreement, which specifies the terms, and conditions under which software may be copied. You must comply with any restrictions.

Virus

- An unauthorized computer software program or portion of a program that has been introduced into a computer or computer system, or network. Viruses damage data files, expand to utilize available space, delete data, or result in other harmful actions.

Appendix B: Technology Responsible Use (Code of Conduct for Students)

The Avon Maitland District School Board will provide students with access to digital technology, access to networks and the Internet. Each student must ensure that they maintain a safe, secure technology footprint and practice good digital citizenship. The purpose of this Code of Conduct for Students is to outline the Boards expectations for technology access for students of the Avon Maitland District School Board.

Personal Safety

1. Students must never give out personal information about themselves or others (such as address, phone number, pictures of themselves) and to strangers met through the Internet.
2. Web pages should not contain personal information about students (address, phone numbers, pictures unless parents have given consent).
3. Students must report to a teacher or other school staff member any technology or Internet related activity (e.g., threats, abusive language) that gives them concern or appears to threaten the safety of people or places.

Use of Equipment, Software and Networks

1. All technology, including cables and network drops, must not be damaged.
2. Use of digital technology including the Internet must respect the safety and rights of others. Information must not be accessed, downloaded, stored or distributed that is illegal, abusive, threatening, obscene, harassing or otherwise inappropriate.
3. Students must not share passwords or use the passwords of others nor should they try to hack into computer systems.
4. Digital data must not be deleted, modified, moved or copied unless permission has been given to do so by a school staff member.
5. Creating and transmitting computer viruses, hoaxes, e-mail worms, sending junk mail or similar nuisance behaviour or related threats to network security is not permitted.
6. Software used must be properly licensed. Licensed software must not be copied illegally.
7. E-mail, conferencing, on-line chat and content of web pages must respect the safety and rights of others.
8. Students must report to a teacher or other school staff member any inappropriate use of digital technology, software or networks, including the Internet.
9. Students must not attempt in any way to log on using another person's identity.
10. Students should not intentionally access Internet sites with inappropriate content of no educational value.
11. If using the work of others, credit must be given and permission obtained if copyright materials are used.
12. Students will only use USB storage devices for transferring school related documents from school to home and vice versa.
13. Students will make every attempt to ensure that the files contained on the USB portable drive are free of viruses, spy ware, and ad ware by having appropriate safe guarding programs on their home computer.
14. Students must not access VPNs or proxy sites that circumvent the security measures put in place by the Avon Maitland District School Board.
15. G-Suite accounts are required for all AMDSB students, regardless of age or grade. Please refer to Appendix D: G-Suite Terms and Conditions

Consequences

Students who do not follow this procedure may be subject to disciplinary action such as loss of computer privileges, disciplinary action and police involvement.

Appendix C: Internet/Intranet Protocol Acceptable Use

The purpose of the board's digital technology, its Local Area Network (LAN), its Wide Area Network (WAN), G-Suite and Internet access is to facilitate communication in support of research and education, by providing access to unique resources and opportunities for collaborative work. The use of any technology and G-Suite must support the educational objectives of Avon Maitland D.S.B. All use of technological resources must comply with existing rules, laws and Acceptable Use procedures found under the Information and Resource conference. The provisions outlined in AP 140 Technology: Responsible Use and Security apply when using G-Suite both during and outside regular working hours.

Electronic Mail

The primary purpose is to conduct Avon Maitland D.S.B. business through cost-effective and efficient communication between and among schools and the corporate headquarters. For example, G-Suite can reduce "turnaround time" on information requests and reduces costs of paper, photocopying, courier delivery etc.
It is not appropriate to send messages to multiple mailboxes including several mailing lists at one time.

Personal Mailboxes

New users to G-Suite are expected to change their password immediately upon activation of their account. Avon Maitland D.S.B. does not assume responsibility for lost messages.

Staff

All staff members are eligible, and are expected to use G-Suite for communication to streamline workflow. Training and manuals for G-Suite are available on a regular basis through the Information Technology Team or by visiting www.iAMgafe.ca
All new account and technical assistance requests should be directed through an eBase IT Work Order.

Non Staff Users

School-based social workers and other support agencies or persons are allowed access to facilitate communication with the schools.

AMDSB Google Groups

The primary purpose of Google groups is the constructive exchange of work-related information broadly within a specific group, and therefore most groups should be "open". Groups are NOT intended for private information; necessary communication of such should be through personal e-mail only. The ultimate decision as to which Google groups are "open" or "closed" rests with the Director of Education or designate. Changes to Google groups are to be directed via the Information Technology Department eBase IT Work Order system.

Union Google Groups

This is a public group and it is appropriate for federation members and management to post any information pertaining to a federation group. Any campaign information is to be posted to these groups **only** for the duration of the campaign. Those posting information during this time are asked to remove messages following the elections.

The Core: Information and Resources

The purpose of this service is to simplify the process of communication of on-going and routine information. Within this website all board policies, administrative procedures, memoranda, forms and templates, as well as current contact information is posted. All information is current and easily available to all employees from any web browser.

Home Usage

The Core and G-Suite are cloud-based services available on most devices via an Internet browser.

Appendix D: G-Suite Terms and Conditions

To support 21st century skills and competencies, students and staff will be supplied with a G-Suite account through the AMDSB domain: ed.amdsb.ca

G-Suite is a set of online tools for communication, collaboration, and time-management and document storage. Google continues to add new tools and AMDSB will evaluate each for its educational potential.

Our primary reasons for supplying these tools to students are:

- To give our students practice in using current technology applications and tools.
- To give students the ability to work on common, no-cost tools on their own documents both at school and outside of school.
- To facilitate “paperless” transfer of work between students and teachers.
- To provide adequate unlimited long-term storage space for student work.
- To allow students to author and/or maintain a portfolio of their learning.
- To help students work collaboratively, engage in peer-editing of documents, and publish for a wider audience.

To provide access to myBlueprint (course & career education planning resource).

Staff will make every reasonable effort to monitor student conduct related to class content in order to maintain a positive learning community. All participants will respect the teacher’s time and professionalism by supporting the same positive approach.

The use of G-Suite is strictly for school purposes only. Any work posted to the site will remain there until removed by the teacher or the student who created it. Students are responsible for managing any personal work posted to their G-Suite account. Students moving to another school board are responsible for transferring their documents to a regular G-Suite account, as their AMDSB G-Suite account will be deleted. G-Suite Accounts for students graduating from AMDSB will remain active for three years after graduation and then graduates will need to transfer their documents to a regular Gmail account.

No student, or other participant, may include any information or images on the site that could compromise their safety or the safety of other class members. Participants should avoid specific comments about our location or schedules, if they would be visible to outsiders.

All participants must protect their login and password information. If participants suspect that a password has been compromised, they must notify the teacher immediately.

All use of these services must be in accordance with the Avon Maitland District School Board’s Responsible Use Policy, including entries made from computers outside of school.