APPENDIX F

Information Technology Security Procedure

Procedure Number:	5017a ~~1. 1.0~~
Procedure Owner:	Information Technology Services
Effective Date:	2013 November 12
Amendment Dates:	2015 November 10 Replaced Procedure #9003 Technology Security Procedures (1998 December 11, 2001, June 13, 2002 February 26, 2007 November 13, 2008 May 27)
EIE Review Date:	2024 December 18
Resources:	• TVDSB Information Technology Policy (5017) • TVDSB Information Technology Appropriate Usage and Electronic Monitoring Procedure (5017b) • Municipal Freedom of Information and Protection of Privacy Act • Ontario Human Rights Code • Canadian Charter of Rights and Freedoms • Canada's Anti-Spam Legislation (CASL) • TVDSB Privacy and the Management of Personal Information Procedure (2014b)

~~Purpose~~

~~To~~

1. Intent

1.1. This procedure specifies the steps Thames Valley District School Board (TVDSB) will take to safeguard its Information Resources and ensure appropriate usage of these resources.

2. Definitions

2.1. **Business Continuity** refers to the ability of an organization to maintain essential

functions and operations during and after a disruptive event, such as a natural disaster, cyberattack, or system failure. In technical terms, business continuity involves the creation of a Business Continuity Plan (BCP), which includes strategies for data backup, system redundancy, disaster recovery, and alternative communication methods. It focuses on minimizing downtime, ensuring access to critical applications and services, and maintaining the integrity of business processes.

2.1. **Cyber Awareness** is the knowledge and understanding of potential cyber threats, such as phishing, social engineering, and data breaches. It involves staying informed about the latest cyber threats that TVDSB and its information resources face every day, following cyber protection best practices, and recognizing the risks associated with common internet activities.

2.2. **Cyber Incidence Response Plan** is the set ~~forth expectations~~of procedures that combines TVDSB processes, resources and technologies for detecting and responding to cyber threats, security breaches or cyberattacks.

2.3. **Cyber Protection** is the term used to collectively describe Cyber Security, Cyber/Online Safety and Digital/Online Privacy.

2.4. **Cyber/Online Safety** refers to the promotion of safe online practices and the mitigation of the risks associated with the inappropriate use of technology in accordance with TVDSB's Appropriate Usage and Electronic Monitoring Procedure.

2.5. **Cyber Security** refers to the protection of information and information technology resources with respect to confidentiality, availability and integrity, and secure network-connected technology resources.

2.6. **Cyber Threat** is any malicious act that seeks to damage data, steal data, disrupt digital life in general or impact TVDSB operations. Cyber threats include computer viruses, malware, data breaches, Denial of Service (DoS) attacks, and other attack vectors.

2.7. **Data Loss Prevention (DLP)** is a set of strategies and tools used to protect sensitive information ~~resources security~~ from being accidentally or intentionally lost, stolen, or exposed. It helps ensure that important data, like personal details, financial information, or confidential documents, doesn't leave the company or organization without permission. DLP can track, monitor, and block any attempts to transfer or access this sensitive data in ways that could put it at risk.

2.8. **Digital/Online Privacy** refers to the protection of personal information, personal health

information, and other TVDSB sensitive information from unauthorized access, and recognizes the importance of guarding personal and sensitive information when using technology.

2.9. **Disaster Recovery Plan (DRP)** is a comprehensive set of procedures and ~~the role and responsibilities of each~~strategies designed to restore IT systems, applications, data, and infrastructure after a disruptive event, such as hardware failure, cyberattack, or natural disaster. It outlines the processes for backing up data, recovering servers, re-establishing network connectivity, and ensuring business continuity with minimal downtime.

2.10. **Information Resources** include but are not limited to TVDSB's information technology services, TVDSB assigned email and network accounts, electronic data, application systems, facilities, wired and wireless networks, and technology equipment and infrastructure that TVDSB owns, operates, or sources from external parties, for the use of students, employees and other authorized users.

2.11. **Multi-Factor Authentication (MFA)** is a security process that requires two or more types of identification before access to an account or system is provided This adds extra layers of protection to make it harder for someone to access a user account.

2.12. **Penetration Testing** is a "security check-up" for computer systems or networks. It involves simulating a cyberattack to find weaknesses or vulnerabilities that could be exploited by hackers. Skilled testers try to "break into" the system, just like a real attacker would, to see where the security could be improved. This helps organizations fix potential problems before a real threat can take advantage of them.

2.13. **Personal Information (PI)** refers to recorded information about an individual ~~in maintaining a secure computing~~that renders that individual identifiable. PI includes name, address, phone number, race, ethnic origin, religious or political beliefs or associations, age, sex, sexual orientation, mental status, family status, any identifying number or symbol such as Social Insurance Number (SIN), fingerprints, blood type, or inheritable characteristics, medical history, educational, financial, criminal, or employment history, personal views or opinions, except if they are about someone else; or anyone else's opinion about that individual.

2.14. **Service Level Agreement (SLA)** is a contract between a service provider and TVDSB that outlines the services to be provided, how performance will be measured, and what happens if the service provider doesn't meet their obligations.

APPENDIX F

2.15. **Single Sign-On (SSO)** is an authentication method that allows users to log in to multiple applications and websites with one set of credentials. Once logged in to one system, users are automatically authenticated for other connected systems without needing to re-enter their login credentials.

2.16. **Software Applications and Systems** safeguard the online privacy and security of students and staff, TVDSB has implemented an approval process to ensure all digital resources meet stringent criteria for safety and educational relevance. The approved resources listed in the Approved Software and Websites have undergone comprehensive evaluation based on their alignment with curriculum objectives, as well as adherence to strict standards for security and privacy protection.

2.17. **Threat Landscape** is a comprehensive overview of all known and potential cyber threats that could affect TVDSB Information Resources, student, employee and other authorized TVDSB users. It includes both current and historical threats, as well as emerging trends, vulnerabilities and exploits.

2.18. **Virtual Private Network (VPN)** establishes a digital connection between a computer and a remote server, creating a point-to-point tunnel that encrypts data, masks an IP address, and avoids website blocks and firewalls on the Internet.

2.19. **Vulnerability Assessments** are a process of checking and identifying weaknesses or security gaps in a computer system, network, or software. The goal is to find areas that could be exploited by hackers or lead to problems like data breaches or system failures. Once these weaknesses are found, steps can be taken to fix or improve them, making the system safer and more secure.

2.20. **Commercial Electronic Message** encourage participation in a commercial activity, including:

2.20.1. Offers to purchase sell, barter or lease a product, goods, a service, land or an interest or right in land

2.20.2. Offers to provide a business, investment or gaming opportunity.

2.20.3. Advertises or promotes anything referred to in (a) or (b); or

2.20.4. Promotes a person, including the public image of a person, as being a person who does anything referred to in (a) or (c), or intends to do so.

Commercial electronic message can be sent via email, SMS text message or instant messaging. It does not include two-way voice communication, a fax, a telephone voice

recording, a social media post or a website post.

2.21. **Commercial Activity** means any particular transaction, act, or conduct or any regular course of conduct that is of a commercial character, whether the person who carries it out does so in expectation of profit.

Exclusions under the Act include commercial activities for the purposes of law enforcement, public safety, protection of Canada, the conduct of international affairs, the defense of Canada, soliciting contributions for a political party/organization/candidate, or fundraising by a registered Canadian charity.

3. Objective of Procedure

3.1. The following objectives help create a secure and resilient Information Technology (IT) environment~~. Since~~ that supports the educational mission of TVDSB while protecting the privacy and safety of all students and staff ~~have~~.

3.1.1. Protecting Student and Staff Data: Safeguarding personal and sensitive information from unauthorized access, breaches, and cyber threats.

3.1.2. Ensuring Cyber Safety: Promoting safe online practices and the mitigation of the risks associated with the inappropriate use of technology in accordance with the TVDSB's Information Technology Appropriate Usage and Electronic Monitoring Procedure.

3.1.3. Compliance with Regulations: Adhering to ~~computer~~local, provincial and ~~Internet resources~~federal laws, as ~~part of their teaching/learning/work experience, they each have a role in maintaining a secure computing environment. Principals and~~ well as TVDSB guidelines and educational standards, to ensure legal and ethical management of data.

3.1.4. Cyber Incident Response: Establishing protocols for responding to cyber incidents, including detection, reporting, and remediation.

3.1.5. Cyber Risk Management: Identifying, assessing, and prioritizing risks to minimize, monitor, and control the probability or impact of adverse events.

4. Roles and Responsibility

4.1. **Staff Supervisors** are accountable for ensuring staff are informed of the procedures and that compliance occurs. All staff members and Trustees are required to complete an annual declaration acknowledging awareness of and the need for compliance with the

Information Technology Policy and underlying procedures.

4.2. ~~personnel~~**Information Technology Services (ITS) Department** will configure, maintain and manage the Information Technology (IT) infrastructure and Information Resources entrusted to its care in accordance with departmental protocols. The ITS department shall establish and maintain cyber protection initiative for implementing and improving cyber security across TVDSB.

4.3. **Contracts and service level agreements** (SLA) with third party service providers who have access to or share custody of the TVDSB Information Resources shall include the obligation to follow the requirements of this procedure as applicable. This shall extend to any subcontractors on whom the service providers rely on to deliver services to TVDSB.

~~1.1.~~4.4. **All users of TVDSB Information Resources** are responsible for ~~communicating expectations and ensuring compliance with safe computing practices as outlined in this document~~ensuring that these resources and the data owned by TVDSB are used exclusively to support TVDSB objectives and in compliance with all applicable local, provincial and federal laws, guidelines and directives. Failure to comply with this Procedure will result in disciplinary action that may include dismissal.

~~2.~~5. ~~Questions or concerns should be addressed through the appropriate supervisor or the Manager of~~ Information Technology ~~Services.~~Security Procedures

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

~~3. 2.0 Background~~

~~The Thames Valley District School Board (the "Board") has responsibility for securing its computing systems against unauthorized access and/or abuse while making them accessible for authorized and legitimate uses.~~

~~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. Because computers throughout the organization are increasingly interconnected, it is essential that responsible security practices be observed to protect the integrity of information stored in computers in schools and administration facilities. Individuals and the Board may be held liable in the event that software is not licensed or properly authorized.~~

APPENDIX F

Administered By	**ASSOCIATE DIRECTOR - LEARNING SUPPORT SERVICES**
Amendment Date(s)	2015 Nov 10
	Replaced Procedure #9003 Technology Security Procedures

Everyone has a part in maintaining a secure computing environment and is expected to adhere to the procedures outlined in this document. This includes students and staff, as well as external agencies and vendors, who have need to use TVDSB networks and technology. Practices have been identified to promote proper password management, Internet access and responsible use of shared resources.

3.0 Principles

3.1 The Board's Information Resources are a Board resource with substantial value that must be protected from inappropriate use, unauthorized modification, destruction or disclosure, whether intentional or inadvertent.

3.2 Access to Confidential Information is restricted to those with a demonstrated "need to know" to the extent required to perform job functions, and must be in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

3.3 The Board must ensure that access to confidential Board electronic information is granted only to appropriate individuals and work groups.

3.4 All Users of the Board's Information Resources must ensure that critical data are securely managed throughout the data life cycle and securely backed up as appropriate.

3.5 Information and equipment disposal practices ensure the continued protection of privacy.

3.6 Systems will be in place to enable the monitoring and detection of inappropriate activity, and the creation of transaction trails for audit purposes.

3.7 Software and its related intellectual property developed by employees in the performance of their duties are the property of the Board, and may not be distributed or shared unless authorized in writing by the Director of Education or designate.

3.8 All software resident on the Board's computers must be installed in compliance with licensing requirements of the software's owners and with Board standards.

3.9 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.

5.1. ~~No Expectation of Privacy – Users of the Board's~~With increased reliance on technology, digital processes, and the internet, TVDSB acknowledges that cyber risks can impact all aspects of the organization, including its staff, students, and reputation. Cyber risk management is a crucial practice that aligns cyber security, cyber safety, and digital privacy with its strategic priorities and operational plan initiatives.

5.2. The following sections will outline TVDSB's essential protocols to Information Technology Security, planning and awareness, access and authentication, devices, applications and monitoring.

6. Essential Protocols for Information Technology Security

6.1. ITS Department will implement reliable, enterprise-grade controls for TVDSB network to regulate all traffic within TVDSB network and between TVDSB and external, untrusted entities (e.g., cloud service providers). Additionally, ITS Department will implement protective measures and controls to procure, monitor, and secure endpoint devices.

6.2. ITS Department will implement Data Loss Prevention capabilities to identify, monitor, and protect data in use, in motion, and at rest. Under no circumstances should an employee transfer or back up TVDSB data from their account to a non-TVDSB account.

6.3. When working remotely, TVDSB Information Resources must be treated as confidential and must not be exposed to unauthorized parties, including individuals such as family members.

6.4. ITS Department will implement technologies and policies to block unsolicited and irrelevant electronic messages (such as spam) from accessing the TVDSB email system. Additionally, ITS Department will adjust the current electronic messaging systems, as needed, to restrict bulk commercial messaging originating from the TVDSB network. TVDSB will ensure that the list of approved software identifies and includes software that complies with Canada's Anti-Spam Legislation (CASL) for the purposes of sending commercial electronic messages.

7. Planning and Awareness

7.1. ITS will categorize IT equipment and resources based on their information sensitivity and associated risks. This classification will help determine the necessary safeguards to protect these resources.

7.2. ITS will assess and reassess cyber risks if there are significant changes to TVDSB information technology solutions, or the threat landscape, or when deemed necessary. Depending on the nature of the identified risk, responsibility for its treatment plan and implementation or remediation may reside with ITS, another department, service area, or external third party.

7.3. ITS will use a combination of vulnerability assessments, penetration testing and other industry practices to monitor, assess, test, and address issues related to the security of TVDSB Information Resources.

7.4. For all business and time-critical IT systems, ITS will implement and review its DRP to support business continuity and timely recovery of IT systems in the event of significant service degradation or unplanned outage.

7.5. ITS will ensure that users of TVDSB information technology resources are aware of how to identify and report a cyber incident or breach.

8. Access and Authentication

8.1. In collaboration with Human Resources (HR), ITS will ensure that new hires and individuals in new positions or roles at TVDSB are assigned appropriate privileges, granted access, and provided with security training relevant to their duties before they are given access to TVDSB Information Resources.

8.2. At the time of retirement, resignation, leave, or termination of employment, HR will collaborate with ITS to ensure timely processes are in place to retrieve TVDSB devices as required and disable access to TVDSB accounts and resources.

8.3. TVDSB will ensure regular, and ongoing cyber awareness and data protection training for TVDSB users is provided.

8.4. TVDSB will implement identity and access management programs to ensure that

only authorized individuals have access to TVDSB Information Resources ~~should have no expectation of privacy with respect to any use of the Board's~~.

8.5. ITS will facilitate and prioritize employee SSO functionality wherever possible subject to security, software and operational limitations.

8.6. All staff users will be required to authenticate using an approved MFA application as the primary means of personal authentication.

8.7. All TVDSB wireless access points, network-connected resources, and internally or externally hosted applications (including cloud services) must conform to TVDSB standards, procedures, and guidelines. Unauthorized networks, access points, and unapproved communication tools at TVDSB schools and sites, including unapproved wireless access points, connected devices, equipment, and remote connections.

8.8. Unauthorized wireless access points, connected devices, equipment, and remote connections will be disabled upon discovery.

8.9. ITS Department is responsible for configuring managing and administering all TVDSB wired and wireless networks. Access to these networks will be restricted to authorized users.

9. Devices

9.1. Only trusted individuals and devices will be permitted to access TVDSB Information Resources. ~~For greater clarity, the Board has the right, and without the consent of the employee, student, or other User,~~

9.2. Only devices configured and managed through ITS will be permitted on any secured TVDSB infrastructure. Devices that are not configured and managed through ITS and/or do not meet a minimum-security standard will not be allowed to operate on any secured TVDSB infrastructure and will not have access to any data, applications, and systems.

9.3. ITS will maintain an asset inventory to track, administer, replace and report on TVDSB technology infrastructure.

10. Applications

10.1. TVDSB shall take appropriate measures to ensure the confidentiality, integrity, and availability of software applications and systems. Any software applications and systems that do not meet TVDSB standards for privacy, security, and/or data protection, as determined by ITS, will not be authorized for use by students and/or staff.

10.2. Contracts and service level agreements with third-party service providers (including any sub-contractors) who have access to or share custody of TVDSB information, IT systems, and/or other TVDSB technology will include the obligation to follow the requirements of this administrative procedure and applicable TVDSB standards, procedures, and guidelines, or be subject to equivalent industry-based assurances.

10.3. All software must undergo a vetting review process prior to installation to evaluate its pedagogical value, technical compatibility, privacy risks, and security concerns. TVDSB staff are required to use only those applications and software listed in the TVDSB approved software list. Any applications or technologies not included in this approved catalogue are prohibited for use by staff and students on TVDSB devices or infrastructure.

11. Network Monitoring

~~3.1.~~11.1. TVDSB shall ensure process and applications are used to monitor any and all of the aspects of its Information Resources, including, without limitation, reviewing documents created and stored on its computer system, deleting any matter stored on its Information Resources, monitoring websites visited by Users, monitoring chat and news groups, reviewing all material downloaded or uploaded by Users from the Internet, and reviewing e-mail sent and received by Users.

~~4.0 Responsibilities of Users~~

11.2. ~~Primary responsibility for security of system level data is vested with the Supervisory Officer (or delegate)~~ ITS will employ automated detection and response

Page 12 of

capabilities to monitor, detect, and remediate potential or actualized cyber incidents and breaches on TVDSB networks, devices/endpoints, systems/applications, network-connected equipment, and platforms.

12. Monitoring and Review

12.1. The monitoring and review of this Procedure is based on the objectives outlined in Section 3.0.

~~4.1~~ The ITS Department will be responsible for ~~the creation or assembly of the information.~~

~~3.1.1.1.~~ ~~Supervisory Officers, Principals and Managers are accountable for ensuring staff are informed of the procedures and that compliance occurs. New employees are to receive a copy of the Information Technology Security Procedures as part of the hiring orientation. All staff members and Trustees are required to complete an annual declaration acknowledging awareness of and the need for compliance with the Information Technology Policy and underlying procedures.~~

~~4.2 Secondary responsibility for the security of information is vested with Information Technology Services staff who manages information processing, transmission, and storage. Information Technology Services staff will act as Information Custodians. The "Information Custodian" is responsible for receiving, granting or denying,~~monitoring and ~~fulfilling users' requests for protected information on behalf of the information owner. The "Information Custodian" may be granted full authorization to access protected systems and other restricted access material in order to fulfill information requests. While the "Information Custodian" may encounter protected or confidential information, the "Information Custodian" agrees to not access, acquire, use, copy, disclose or transfer this information except to the extent necessary to fulfill the authorized information request. ITS staff will configure, maintain and manage the Information Technology infrastructure resources entrusted to its care in accordance with departmental protocols.~~

~~4.3 Users of the Board's Information Resources are responsible for using Information Resources in accordance with~~reviewing this Procedure ~~and all related policies and procedures, and complying with control and disclosure procedures, as required by MFIPPA. Users' access to the Board's corporate applications will be granted and managed as outlined in departmental~~

protocols.

4.4 Data, computer equipment and software must be protected at all times from physical damage, theft or unauthorized modification by those responsible for its use and physical security.

4.5 Board-owned individually assigned computers must not be left unattended when the power is on and CONFIDENTIAL OR CRITICAL information is being accessed.

4.6 It is recommended that confidential or sensitive information be kept on network drives. Where confidential or sensitive information is stored on Board owned hardware or mobile storage (i.e., memory sticks) or devices every effort must be taken by the user to ensure that the device is physically secure, information is

backed up, and sensitive materials are protected by logical access controls such as passwords and encryption.

There is an obligation to inform parties if there is a privacy breach and confidential personal data is lost or stolen (e.g., on content of laptop hard drive, lost memory stick). This process is outlined in the section entitled "Handling a Privacy Breach" of the #2020.

4.7 Non-Board owned equipment may be used on designated wireless networks within the Board, but may not be attached to wired Board Networks. When non- Board equipment is used on designated wireless networks within the Board, they must still be used in accordance with the Information Technology Policy, the Information Technology Appropriate Usage Procedure and this Information Technology Security Procedure, and any other applicable Board policy or procedure, and any applicable laws.

4.8 Failure to comply with the Information Technology Security Procedures will result in disciplinary action that may include dismissal.

5.0 Technology Security Practices

5.1 Malware Issues

Malware (viruses, spyware, etc.) 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, from infected media and from email attachments or, more rarely, email messages. Viruses can be highly destructive, damaging data and even making an infected computer unusable (e.g., by disabling it from launching any software programs). Virus removal can be difficult and in some cases may necessitate reformatting the hard drive or media resulting in the loss of all data.

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:

- maintain up-to-date anti-virus software; updating software regularly is necessary to obtain protection against the most recent viruses
- use anti-virus software to scan all files downloaded or copied to devices
- ensure that all software has been approved through the Software Approval Committee
- do not open any email messages or email attachments which appear suspicious. 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
- back up important files regularly to minimize data loss should your system become infected with a virus

Common symptoms of virus infection include unusual messages or displays on the screen, missing and inaccessible or unusable files or programs. Individuals are asked to contact the Information Technology Services Help Desk in the case of a suspected virus.

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, increases in email traffic). Individuals who receive virus alerts from persons or organizations outside the Board are asked to forward the information to ITS Help Desk. Often such "alerts" are hoaxes. The Help Desk will research any such information and where appropriate issue genuine virus alerts or warnings.

5.2 Software and Licenses

Software licenses agreements must be honoured even if the software is not copy-protected. All software used for Board operations must be installed in compliance with licensing requirements of its owners or otherwise owned by the Board.

Please contact the Manager of Information Technology Services to find out about terms and conditions of software licenses for administrative applications which are centrally supported. Users must maintain records of legal licenses.

5.3 Hardware

Computer equipment must be located where they will be secure and as free as reasonably possible from damage by water, fire, or other disasters.

Laptops, personal computers, mobile devices and related equipment must be handled securely, as the high value and portability of these devices make them desirable theft items. Mobile devices must not be left unsecured at any time, including in cars or offices.

5.4 Removable Media

Data may be stored on removable media, as well as computer hard drives and servers. Important data must be appropriately backed up. 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 media are stored near magnetic fields (telephones or monitors), mishandled or misused. 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 removable media are not handled safely.

5.5 Contingency Plans/Backup

The school administrator or the Help Desk (519-452-2005) should be contacted for assistance in obtaining alternate means of computing in case of an emergency.

Every department is responsible for contingency planning in the event of an emergency. 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 location other than the computer workstation. A regular routine to perform backups for servers and PC data must be established.

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.

5.6 Password/User Authorization Safety

Passwords belonging to individuals are not to be posted in public access areas or near the computer itself. Keep them in a secure place. Passwords are not to be shared.

In selecting a password, choose something that is known only to you:

- do not use your log-in name in any form (i.e., as-is, reversed, capitalized)
- avoid your first, middle or last name in any form
- do not use the names of your spouse or children
- do not use other information easily obtained about you - including license plate, telephone number, social insurance number, make of automobile, name of street on which you live
- use a password that is easy to remember, so that you do not have to write it down
- consider combining 2 or 3 words together with numbers and use a pass phrase (e.g., Cut73trees)
- avoid using the identical password for multiple purposes as

if this password is compromised it will affect multiple applications

Password length, complexity and lifetime will be enforced as outlined in departmental protocols.

5.7 Data Integrity

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

5.8 Electronic Mail, Conferencing And Other On-Line Communications

The Board may monitor the contents of electronic messages carried on its computer networks. Electronic mail originating from the Board, like traditional mail, is to be used only to further the Board's objectives, and is the Board's property. All communications are to use appropriate and respectful language and to be consistent with the Board's policies and procedures, the *Canadian Charter of Rights and Freedoms*, the *Ontario Human Rights Code*, the *Ontario Occupational Health and Safety Act*, the *Municipal Freedom of Information and Privacy Protection Act*, and any other applicable law.

5.9 Internet Access

The Board provides connections to the Internet for staff and student use that is consistent with Board objectives. Use of the Board's Internet access contrary to Board policies, procedures or applicable laws will result in disciplinary action that may include dismissal.

4. Appendi

x A

DEFINITI

ONS

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

"ACCESS" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

5. "BOARD'S INFORMATION RESOURCES"

Hardware: CPU's, computer boards, keyboards, terminals, workstations, personal computers, printers, mobile devices, disk drives, wired and wireless infrastructure, communication lines,

terminal servers, routers, PDA's laptops, phones and USB flash drives.

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.

"COMPUTER NETWORK" means a number of computers connected together that are capable of sharing common resources such as files, printers and CD Rom services.

"COMPUTER PROGRAM" means a set of instructions that tells the computer what to do.

"COMPUTER SOFTWARE" means programmed instructions whether purchased or written by the user that the computer carries out.

"CONFIDENTIAL" (or SENSITIVE) information is information which requires protection from unauthorized access and is regulated by a policy: for example; personally identifiable student data such as grades and test results.

"CONTINGENCY PLANS" are alternative steps to take when alignment with legislative changes, 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" information, networks, applications, systems, or data, are those resources determined by management to be essential to the Board's critical functions.

"FREEWARE" is software that is available for free use.

"INFORMATION CUSTODIAN" refers to the person(s) responsible for overseeing and implementing the necessary safeguards to protect information assets, at the level classified by the owner of the information.

"INTELLECTUAL PROPERTY" means data, including programs that are subject to copyright protection as "Personal" property or "Board" property.

"INTERNET" is a logical network of tens of thousands of interconnected host computers.

~~**"MALWARE"** or malicious software is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.~~

~~**"PDA"** is personal data assistant.~~

~~**"PERFORMANCE OF THEIR DUTIES"** relates to JOB duties as specified in the employee's JOB DESCRIPTION.~~

~~**"PROPERTY"** means anything of value and 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.~~

~~**"REMOVABLE MEDIA"** includes any media that can be removed from electronic devices, including such items as USB drives, zip drives, DVD/CD drives, external hard drives, etc.~~

~~**"SHAREWARE"** is 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"** is an agreement which specifies the terms and conditions under which software may be copied. You must comply with any restrictions.~~

~~5.1.~~12.2. ~~**"VIRUS"** is 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.~~practices and/or Ministry of Education directives.