Peterborough Victoria Northumberland and Clarington Catholic District School Board

BOARD ADMINISTRATIVE PROCEDURE	
Administrative Procedure **Employee Acceptable Use of Technology**	*Administrative Procedure Number* **511**
Directional Policy **500-Employee Relations**	

Title of Administrative Procedure:

Employee Acceptable Use of Technology

Date Approved:

May 2023

Projected Review Date:

2028

Directional Policy Alignment:

500 Employee Relations

Alignment with Multi-Year Strategic Plan:

This Administrative Procedure informs priorities under the 2021-2025 Strategic Plan, Vision and Mission: *Building a Community That Accompanies*, particularly the goals of Nurturing Mental Health & Well-being, Ensuring Equity and Expanding Technology.

The board is committed to ensuring that technology is used for proper work-related purposes and in a manner that is not detrimental or harmful to the interests of others or that compromise the confidentiality or proprietary nature of information belonging to the Board. The intent is to create a shared understanding of the expectations the Board has with respect to employees' conduct with and via technology.

Action Required:

It is the practice of the Peterborough Victoria Northumberland and Clarington Catholic District School Board to provide authorized employees and service providers with access to the Board's Technology systems, including (but not limited to) its electronic mail, Internet, and voicemail systems.

The Board shall maintain an environment of technologies (hardware, software, databases, applications) that are intended for use, as part of its overall technology platform. The technologies are provided to assist in the conduct of Board business and may be utilized only as directed or outlined by the Board. All email and Internet communications sent and received by users, and data files stored on any board issued technology, shall remain the property of the Board. Employee email, Internet voicemail communications and data files are not private or personal despite any such designation by the sender or the recipient. Personal or private communications transmitted on the Board's electronic information system may be accessed, reviewed, copied, deleted, retained, or disclosed by the Board at any time and without notice. Records created by Board staff in the performance of their duties are subject to the Municipal Freedom of Information and Protection of Privacy Act and may be subject to public disclosure.

The Board reserves the right, without prior notice to the employee, to monitor the Technology systems at the work site. The Board may access any of these technology systems, devices, or networks any time and without prior notice to the employee or service provider. Some staff members have been assigned Board issued technology to help with planning. Staff members are permitted to use board technology for incidental personal use but the board will, nevertheless, retain the right to search the board technology to ensure compliance with this policy, including searching personal files that might be stored on the board hardware.

Failure to comply with this Administrative Procedure may result in the loss of access privileges, financial compensation to the Board, pursuance of criminal charges, and/or other disciplinary action up to and including discharge.

Responsibilities:

The Board of Trustees is responsible for:

- Ensuring alignment with the Employee Relations Directional Policy.
- Reviewing the Employee Acceptable Use of Technology Administrative Procedure as part of its regular policy and procedure review cycle.

The Director of Education is responsible for:

- Designating resources for ensuring the implementation and compliance with this Administrative Procedure.

Superintendents of Schools and System Portfolios are responsible for:

- Supporting implementation of this Administrative Procedure.
- Reviewing and authorizing requests for access to technology systems that support curriculum outcomes but may be outside the stated guidelines of the policy.
- Collecting and returning board technology to IT department within a 2 week period of a staff member commencing a leave of absence or ending an assignment. This 2 week period can be extended by the Superintendent.

Superintendent of Information Technology (or designate) is responsible for:

- Monitoring usage of the board's technology systems and establishing guidelines for IT staff for monitoring.
- Providing digital citizenship and Internet safety resources for employees.
- Providing a unique username and password for each employee for their exclusive access to the Board's technology systems.
- Reviewing requests for technology system that support curriculum to ensure they comply with other administrative procedures and protect the privacy of users consistent with applicable laws and regulations.

Manager of Human Resources is responsible for:

- Ensuring all new staff acknowledge they have read and understood the Administrative Procedure and will place a signed copy of the acknowledgement form in the employee's personnel file. An electronic acknowledgement of the policy may also serve as the official record in lieu of a paper copy.

Principals and Vice-Principals are responsible for:

- Ensuring that on an annual basis each of their staff complete the Employee Acceptable Use of Technology Agreement. An electronic acknowledgement of the administrative procedure may also serve as the official record in lieu of a paper copy.
- Alerting the Superintendent of IT (or delegate) upon learning of misuse of technology systems.
- Collecting and returning board technology to IT department within a 2 week period of a staff member commencing a leave of absence or ending an assignment. This 2 week period can be extended by the Principal.

Staff are responsible for:

- Completing, on an annual basis, the Employee Acceptable Use of Technology Agreement. An electronic version of the agreement may also serve as the official record in lieu of a paper copy.
- Protecting the integrity of their board user account credentials and MFA tokens and being accountable for their use by:

  - Never sharing their password
  - Securely storing MFA and security tokens
  - Not using the same password for work as for personal accounts
  - Not writing down passwords or including them in email
  - Not storing passwords electronically unless encrypted
- Abiding by generally accepted rules of etiquette, including the following:
  - Be polite and respectful. Do not be abusive in your exchanges with others.
  - Use appropriate language. The use of abusive, harassing, or profane language is prohibited.
  - Do not post chain letters or engage in “spamming”.
- Abiding by the following generally accepted rules of etiquette for preventative care of the board issued device:
    - Protect the device from damage or theft.
    - Ensure the device is stored in a safe and secure location
    - Ensuring the correct power adapter is connected
    - Ensure the device is cared for in an appropriate manner:
      - Do not place anything on the keyboard before closing the screen
      - Avoid having food or beverages around the laptop
      - Do not expose the device to extreme hot or cold temperatures
      - Clean the device often, i.e. with a microfiber cloth
      - Do not have any items pressed against the laptop when being stored

- Ensuring only authorized and approved software or applications are installed on board issued devices
- Ensuring your board issued device is only used or accessed by PVNC board staff
- Conserving Internet bandwidth by limiting activities known to consume large amounts of bandwidth
      - e.g. video streaming to multiple individual devices when a single stream to a projector would be more appropriate.
      - e.g. audio streaming during the school day when a radio would be more appropriate.
- Complying with the Board’s Personal Network Device policy if using a Personal device on a Board network, i.e. BYOD
- All devices connecting to the PVNCCDSB Corporate network must be board approved and should be connected to that network wirelessly.
- Devices attached to the PVNCCDSB Corporate network must be approved by the Supervisor of Corporate Systems
- Personal devices connecting to the BYOD network must comply with the Board’s Personal Network Device Policy
- Ensuring that when sending Commercial Electronic Messages that the message is compliant with the Canadian Anti Spam Legislation requirements. The sender of a Commercial Electronic Message must:
    - Have the consent of the recipient
    - Provide their identification, including mailing address
    - Provide a readily available method to unsubscribe

- Alerting their immediate supervisor upon learning of misuse of technology systems.
- It is the employee's responsibility to safeguard student data under the Ontario Student Record Guidelines and if applicable, the Municipal Freedom of Information and Protection of Privacy Act, the Ontario Health Information Protection Act and/or Board Policy 306 - Privacy of Personal Information. Employees who suspect that this data has been compromised shall notify their immediate supervisor.
- Ensuring they do not send confidential or proprietary information to technology systems external to the board, nor forwarding emails marked as confidential. Employees may, with the approval of a Supervisory Officer, exchange proprietary information with an Approved Service Provider over technology systems provided the appropriate level of encryption is in place (in transit and at rest).
- Ensuring they do not establish Internet, external or remote connections that could allow unauthorized access to the Board's technology systems and information.
- Ensuring they do not use technology systems to store, distribute, post, download, or view any defamatory, abusive, obscene, profane, pornographic, sexually oriented, threatening, racially or ethnically offensive, sexist or illegal material.
- Ensuring that their use of technology does not interfere with their work duties and responsibilities.
- Ensuring PVNC technology systems are not used for any unlawful activity that adversely affects someone, such as storing, distributing, posting, downloading, or viewing defamatory, abusive, obscene, profane, pornographic, sexually oriented, threatening, racially or ethnically offensive, sexist, or illegal material. Refer to Appendix A for a detailed list of examples.
- Do not circumvent the Board security systems
- Ensuring board issued technology is returned to their immediate supervisor if going on a leave (greater than 2 weeks) or ending a work assignment.

Students are responsible for:

- X

Parents are responsible for:

- X

Progress Indicators:

- Completion of Acceptable Use Agreement at time of hire and annually thereafter
- Results of IT and Security audits

Definitions:

- **Approved Service Provider** – An organization that provides educational or ancillary services to the Board, for example, a transportation consortium.
- **Commercial Electronic Message (CEM)** - an electronic message that encourages participation in a commercial activity, including, but not limited to: offering, advertising or promoting a product, a service or a person.
- **Employee** - a person who performs any work for, or supplies any services to, an employer for wages (excluding honoraria).
- **Personal Network Device** - a device, owned by the user, which has the capability to connect to a computer network, either through a network wire or using a radio designed to connect to a wireless computer network. Examples include: laptops, netbooks, some portable music players, some portable game devices, and most cellular telephones.
- **Spamming** - sending an annoying or unnecessary message to a large number of users.
- **Technology Systems** - all forms of technology used to create, store, exchange and use digital information in its various forms (data, audio, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).
- **Unlawful Activity** - Appendix 'A'

References:

- PVNC Catholic District School Board Vision and Strategic Priorities 2021-2025
- Employee Relations Directional Policy - 500
- Personally Owned Network Device Policy - 904
- Privacy of Personal Information Policy - 306
- Canadian Anti-Spam Legislation
- Municipal Freedom of Information and Protection of Privacy Act
- Ontario Student Record Guidelines
- Ontario Personal Health Information Protection Act
- Ontario Libel and Slander Act

APPENDIX A - Unlawful Activity

For the purpose of this policy, “unlawful activity” is interpreted broadly and includes any criminal activity or other illegal activity.

The following are examples of ‘unlawful activity” for the purpose of the policy:

Child Pornography	possessing, downloading or distributing and child pornography
Intellectual Property	infringing on another person’s copyright, trademark, trade secret of any other property without lawful permission. This includes possession of tools to defeat intellectual property controls (i.e. key generators and cracking software)
Other Criminal Activity	using electronic transmissions as a means to commit criminal activity (i.e.examples include but not limited to fraud, extortion, sale and /or purchase of restricted goods)
Defamation Libel	A matter published without lawful justification or excuse, that is likely to injure the reputation of any person by exposing that person to hatred, contempt or ridicule, or that is designed to insult the person - The libel and Slander Act, RSO 1990, Chapter L.12.
Disclosing or Gathering Personal Information	Disclosing personal information in a manner inconsistent with the Municipal Freedom of Information and Protection of Privacy Act.
Hacking and other crimes related to computer system	Examples include (but are not limited to): - gaining unauthorized access to a computer system - trying to defeat the security features of network connected devices - use of software and/or hardware designed to intercept, capture and/or decrypt passwords - intentionally spreading a computer virus - destroying or encrypting data without authorization and with the intent of making inaccessible to others’ with a lawful need to access it. - interfering with other’s lawful use of data and technology.
Harassment	engaging in a course of vexatious comment or conduct against a person that is known or ought reasonably to be known to be

	unwelcome, including by electronic means.
Hate Propaganda	communicating messages that promote or incite hatred against an identifiable group that is likely to lead to a breach of the peace.
Interception of private communications or electronic mail	unlawfully intercepting someone’s private communications or electronic mail.
Obscenity	distributing, publishing or possessing for the purpose of distributing or publicly displaying and obscene material.