CATHOLIC DISTRICT SCHOOL BOARD OF EASTERN ONTARIO
www.cdsbeo.on.ca

BOARD ADMINISTRATIVE PROCEDURE

ADMINISTRATIVE PROCEDURE

801 Employee Acceptable Use of Technology

DIRECTIONAL POLICY

Nurturing Employee Relations

Title of Administrative Procedure:

Employee Acceptable Use of Technology

Date Approved:

October 2022

Projected Review Date:

October 2027

Directional Policy Alignment:

This Administrative Procedure aligns with the Nurturing Employee Relations Directional Policy, by establishing guidelines for employees regarding acceptable use of technology, while supporting our moral purpose and the Board vision of transforming the world with justice and peace through Catholic education, inspired by the teachings of Jesus Christ.

Alignment with Multi-Year Strategic Plan:

This policy aligns with the Multi-Year Strategic Plan objective of **Protecting**. Specifically, the Priorities of:

- Foster safe learning environments that ensure the mental and physical health of our students as a priority.
- Set priorities for the use of fiscal resources which are consistent with the Board's Vision and Mission statements, and comply with the Ministry of Education's mandates, regulations, and guidelines.

The alignment with these priorities is to ensure that the Board has clearly outlined the requirement for the acceptable use of board technology assets and systems for our employees. 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 our students, staff, parents, or any other stakeholder. As well that its use does not 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 employee conduct with and via technology.

CDSBEO Strategic Plan 2020-2025

Action Required

It is the practice of the Catholic District School Board of Eastern Ontario to provide authorized employees and service providers with access to the Board's Technology systems, including (but not limited to) its electronic messaging, internet, electronic file storage, and voice mail systems.

The Board shall maintain electronic messaging, internet, electronic file storage, and voice mail systems as part of its technology platform. These systems are provided to assist in the conduct of Board business and may be utilized only as directed or outlined by the Board. All messaging and internet communications sent and received by users utilizing board technology shall remain the property of the Board. Employee electronic messaging, internet, electronic files, or voice-mail communications 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, online services, devices, or networks any time and without prior notice to the employee or service provider. 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 technology hardware, services, or systems.

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.

This Policy shall be read and interpreted to be in alignment with, and subject to the Municipal Freedom of Information and Protection of Privacy Act.

Responsibilities

The Board of Trustees is responsible for:

- 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 supports curriculum outcomes but may be outside the stated guidelines of the policy.

Manager of Information Technology 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.

Manager of Human Resources is responsible for:

- Ensuring all new staff acknowledge they have read and understood the Administrative Procedure. 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.
- Providing access to the Administrative Procedure at the work site and, upon request of an employee, will provide a personal copy of the Administrative Procedure.\

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 being accountable for their use by:

  - Never sharing their password
  - Not using the same password for work as for personal accounts
  - Not writing down passwords or including them in email
  - Not storing password electronically unless encrypted
- Abiding by generally accepted rules of etiquette, including the following:
  - Being polite and respectful. Not being abusive in exchanges with others.
  - Using appropriate language. The use of abusive, harassing, or profane language is prohibited.
  - Not posting chain letters or engaging in "spamming"
- Conserving internet bandwidth by limiting activities known to consume large amounts of bandwidth such as the following examples:
  - video streaming to multiple individual devices when a single stream to a projector would be more appropriate.
  - audio streaming during the school day when a radio would be more appropriate.
- Complying with the Boards Use of Personally Owned Computers policy if using a Personal Network Device. CDSBEO Procedure F1:3 Use of Personally Owned Computers
- 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 on the work site.
- From time to time, staff will have in their possession electronic versions of student data. It is the employee's responsibility to safeguard that data under the Ontario Student Record Guidelines and, if applicable, the Municipal Freedom of Information and the Protection of Privacy Act, the Ontario Health Information Protection Act and/or Board Policy F2: Freedom of Information and Protection of Policy.
- Ensuring 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 or implied as confidential in nature. 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 or external connections that could allow unauthorized access to the Board's computer systems and information. These connections include (but are not limited to) the establishment of multi-computer file systems, ftp servers, email servers, telnet, internet relay chat or remote-control software.
- 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.
- Adhering to the boards Procedure F4:6 Use of Electronic Communications and social media as well as the CDSBEO Social Media Guidelines for Employees.
- Ensuring that their use of technology does not interfere with their work duties and responsibilities.
- Ensuring technology systems at a work site are not used for any unlawful activity as outlined in Appendix A.

Progress Indicators

- Mutual understanding and awareness of the expectations and responsibilities staff have in the use of Board technology systems and services.
- 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 the Board for wages (excluding honoraria).
- **Service Provider** – a person who supplies any services to the Board for a fee.
- **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

- CDSBEO Procedure F1:3 Use of Personally Owned Computers
- CDSBEO Procedure F2:1 Freedom of Information and Protection of Privacy
- CDSBEO Procedure F2:2 Ontario Student Records
- CDSBEO Procedure F2:7 Canada's Anti-Spam Legislation
- CDSBEO Procedure 601 Electronic Monitoring
- CDSBEO Procedure F4:6 Use of Electronic Communications and Social Media
- CDSBEO Social Media Guidelines for Employees
- 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 unlawful activity.

The following are examples of "**unlawful activity**" for the purpose of the policy, but are not intended to be an exhaustive list of such activities:

Child pornography: possessing, downloading, or distributing any 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 (e.g., key generators and cracking software).

Other Criminal Activity: using electronic transmission as a means to commit criminal activity (examples include but are not limited to fraud, extortion, sale and/or purchase of restricted goods)

Defamatory 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 it 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 any obscene material.