Northeastern Catholic District School Board

RESPONSIBLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY

Administrative Procedure Number: API002

POLICY STATEMENT

The Northeastern Catholic District School Board (NCDSB) recognizes that Information and Communication Technology (ICT) is essential to teaching, learning, communication, and the effective operation of the Board. The Board is committed to providing secure, reliable, and equitable access to technology resources that support student achievement, innovation, and responsible stewardship.

The Board believes that technology must be used in ways that are ethical, responsible, and consistent with Catholic teachings. NCDSB is committed to fostering responsible digital citizenship, protecting the privacy and dignity of all individuals, and promoting the appropriate use of emerging technologies, including artificial intelligence (AI), in support of learning and the Ontario Catholic School Graduate Expectations.

REFERENCES

Catholic Curriculum Corporation
- *Ethical and Responsible Use of Information and Communication Technology*

Ontario College of Teachers: *Effective Use of Technology*
Municipal Freedom of Information and Protection of Privacy Act
NCDSB AI Guiding Principles
NCDSB Board Policy
- C-2 Communication with the Public
- E-24 Personal Information Management
- E-29 Borrowing of Board Owned Equipment and Technology
- I-2 Responsible Use of Information and Communication Technology
- I-3 Electronic Monitoring
- I-6 Hand-Held (Mobile) Wireless Communication Device

DEFINITIONS

Artificial Intelligence
Computer systems or applications that generate or analyze content, assist with decision-making, or perform tasks that typically require human intelligence. AI tools must be used in a manner that is ethical, responsible, and consistent with Board policies, administrative procedures, and applicable legislation.

Board Technology Resources
All technology owned, leased, licensed, or provided by the Board, including devices, networks, internet services, software, applications, cloud-based services, email systems, digital learning platforms, and

electronic information.

Digital Citizenship
The safe, ethical, respectful, and responsible use of technology that reflects good judgment, protects the dignity and privacy of others, and supports positive participation in digital environments.

Information and Communication Technology (ICT)
The Board's technology resources used to create, access, store, process, communicate, secure, or share information. ICT includes hardware, software, networks, internet and cloud-based services, communication systems, applications, electronic mail, digital learning platforms, and related technologies used by or on behalf of the Board.

Personal Information
Has the same meaning as defined in the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Personal Network Device
A device, owned by a 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, net books, portable game devices, and cellular telephones.

Responsible Use
The ethical, lawful, and secure use of Board technology resources, systems, networks, devices, applications, and information in support of learning, teaching, administration, and other authorized Board purposes. Appropriate use includes compliance with applicable legislation, Board policies and administrative procedures, and respect for the privacy, safety, security, and dignity of all members of the school community.

User
Any individual who accesses or uses Board Technology Resources, including students, staff, trustees, volunteers, contractors, parents/guardians, visitors, and other authorized individuals.

PROCEDURES

1.0 GENERAL PROVISIONS

1.1 Users are responsible for their own online activities and decision-making when using Board-approved technology resources. If inappropriate content bypasses the Board's security and filtering systems, users must immediately stop accessing the content and report the incident to a staff member, supervisor, or the ICT Department, as appropriate.

1.2 All users must:

i) Use technology for educational, professional, or board-approved purposes.

ii) Protect personal information and respect the privacy of others.

iii) Use only their assigned accounts and keep passwords confidential.
iv) Access only authorized systems, data, and resources.
v) Report security concerns, suspicious activity, or breaches immediately.
vi) Follow all applicable laws, including copyright, privacy, and anti-harassment legislation.
vii) Use respectful, appropriate communication in all digital interactions.
viii) Use Board technology primarily for educational or work-related purposes.

1.4 Users must NOT:

i) Access, create, store, or distribute inappropriate, offensive, or harmful content.
ii) Attempt to bypass security controls, filters, or monitoring systems.
iii) Install unauthorized software or hardware.
iv) Engage in cyberbullying, harassment, or discrimination.
v) Use Board-approved technology for personal financial gain, political campaigning, or illegal activity.
vi) Damage, modify, or interfere with Board systems or devices.

2.0 ROLES & RESPONSIBILITIES

2.1 ICT Department

The ICT Department is responsible for:

i) Maintaining secure, reliable technology infrastructure.
ii) Monitoring the systems and services provided to end users for usage and availability.
iii) Implementing cybersecurity measures, filtering, and monitoring systems.
iv) Managing user accounts, permissions, and access levels and ensure they are placed in the proper access groups.
v) Providing technology systems and services to staff and students and set standards for their use.
vi) Providing technical support and training.
vii) Deploying and configuring Board-approved devices, ensuring they are securely configured, regularly updated, and compliant with Board standards and Ministry of Education requirements.
viii) Investigating reports of misuse and documenting incidents.
ix) Ensuring compliance with privacy legislation and Board policies.
x) Notifying the appropriate Supervisory Officer of suspected inappropriate activities, security incidents, or access to inappropriate content.
xi) Securely disposing of obsolete systems and devices, ensuring that all storage media are sanitized or destroyed in accordance with Board standards.

ICT Department must NOT:

i) Access user files or communications without proper authorization or legal justification.
ii) Provide support to non-Board provisioned systems or services.

iii) Provide technical support for non-Board-approved devices, systems, applications, or services.
iv) Configure or support personal devises for access to the NCDSB wi-fi network, except where expressly authorized by a Supervisory Officer.

2.2 Supervisory Officers

Supervisory Officers are responsible for:

i) Ensuring schools and departments comply with this Administrative Procedure and related NCDSB policies governing the acceptable use of technology.
ii) Supporting Principals and Managers in responding to incidents involving misuse of technology or inappropriate access to digital content.
iii) Collaborating with the Manager of ICT to determine an appropriate response to reported incidents involving inappropriate technology use, cybersecurity concerns, or access to inappropriate content, taking into consideration the circumstances of each case.
iv) Approving technology initiatives or exceptions within their area of responsibility, where appropriate and in accordance with NCDSB policy.
v) Supporting the implementation of professional learning that promotes digital citizenship, cybersecurity awareness, and the safe, ethical, and responsible use of technology.

2.3 Principals and Managers

Principals and Managers are responsible for:

i) Communicating the expectations outlined in NCDSB Policy I-2 *Responsible Use of Information and Communication Technology* and this administrative procedure to staff, students, and where appropriate, parents/guardians.
ii) Ensuring appropriate supervision of student technology use and promoting the safe, ethical, and responsible use of technology.
iii) Reporting and documenting suspected misuse of Board technology resources in accordance with NCDSB procedures and notifying the appropriate Supervisory Officer.
iv) Collaborating with Manager of ICT and the appropriate Supervisory Officer in investigation and resolution of technology-related incidents.
v) Implementing appropriate corrective or disciplinary measures in accordance with NCDSB policies, applicable legislation, and collective agreements where required.
vi) Ensuring the annual compliance of technology agreements at the beginning or each school year.
vii) Ensuring compliance to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and other privacy legislation by protecting the confidentiality and security of student and staff personal information.
viii) Promoting and monitoring staff compliance with NCDSB expectations for the appropriate, professional, and secure use of technology, including digital communication tools and social media.

2.4 Staff

Staff are responsible for:

i) Modeling appropriate digital citizenship and the safe, ethical, and responsible use of technology.

ii) Supervising and managing student use of technology and digital resources, where applicable, in accordance with their assigned responsibilities.

iii) Using only Board-approved technology, systems, applications, and digital tools that comply with Board privacy, cybersecurity, and safety requirements.

iv) Prompt reporting suspected technology misuse, cybersecurity incidents, or safety concerns to their Principal, Manager, or Supervisor.

v) Using Board technology resources in support of their professional responsibilities in accordance with NCDSB policies and administrative procedures.

vi) Protecting the privacy and confidentiality of student, staff, and Board information by complying with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and other applicable legislation and Board requirements.

Staff must NOT:

i) Use personal accounts or unauthorized applications, systems, or services to conduct Board business or support student learning, unless expressly approved by a Supervisory Officer.

ii) Share, disclose, or store confidential student, staff, or Board information using unapproved platforms or methods.

2.5 Students

Students are responsible for:

i) Using Board technology resources in support of their learning and other school-related activities.

ii) Protecting the confidentiality of their passwords and use only their own Board-issued accounts.

iii) Demonstrating respectful, responsible, and safe digital citizenship in all online interactions.

iv) Promptly reporting inappropriate content, online behaviour, security concerns, or suspected misuse of technology to a staff member.

Students must NOT:

i) Engage in cyberbullying, harassment, discrimination, or other inappropriate or unsafe online behaviour.

ii) Access, attempt to access, or distribute inappropriate, illegal, or harmful content, or attempt to bypass Board security of filtering systems.

iii) Damage, misuse, or tamper with Board technology resources, devices, networks, software, or security settings.

iv) Capture, share, or distribute photographs, videos, recordings, or personal information of others without appropriate permission or authorization.

2.6 Other Authorized Users
(Contractors, Parents/Guardians, Trustees, Visitors, Volunteers)
Other Authorized Users are responsible for:

i) Using Board technology resources only for authorized Board-related purposes.
ii) Complying with all applicable NCDSB policies, administrative procedures, and technology-related privacy, safety, and cybersecurity requirements.
iii) Promptly reporting suspected technology misuse, security incidents, or other concerns to the school principal, site supervisor, or appropriate Board contact.

Other Authorized Users must NOT:

i) Access, use, or disclose confidential student, staff, or Board information unless expressly authorized to do so.
ii) Install software, connect unauthorized devices, or attempt to modify Board technology resources, systems, or networks without approval.

3.0 REPORTING, INVESTIGATION AND RESPONSE

3.1 Reporting Concerns

3.1.1 Any individual who becomes aware of the inappropriate use of Board technology resources, a suspected cybersecurity incident, unauthorized access to Board systems or information, or any activity that may compromise the security, privacy, or integrity of Board technology shall report the matter as soon as reasonably possible.

3.1.2 Reports shall be directed to the appropriate individual, depending on the nature of the concern:

i) **Students** shall report concerns to a staff member.
ii) **Staff** shall report concerns to their Principal, Manager, or Supervisor.
iii) **Principals and Managers** shall notify the appropriate Supervisory Officer and the ICT Department, as required.
iv) **Technical or Cybersecurity incidents** shall be reported immediately to the ICT Department.
v) **Serious Incidents** involving potential legal, privacy, or safety concerns shall be referred to the appropriate Supervisory Officer.

3.1.3 All reports will be treated confidentially to the extent possible and in accordance with applicable legislation and Board policies.

3.2 Investigation and Response

3.2.1 Reports of suspected misuse will be reviewed and investigated in a timely, fair, and confidential manner, consistent with applicable legislation, Board policies, administrative procedures, and collective agreements, where applicable.

3.2.2 Depending on the nature and severity of the incident, the Board may:

i) Assess and investigate the reported concern.

ii) Preserve relevant electronic records or digital evidence.

iii) Involve the ICT Department, school administration, Human Resources, Supervisory Officers, or other appropriate Board personnel.

iv) Notify parents/guardians when incidents involve students, where appropriate.

v) Respond to privacy breaches in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), other applicable legislation, and NCDSB policies.

vi) Refer matters to law enforcement or other authorities where criminal activity or other legal obligations may exist.

3.3 Corrective and Disciplinary Measures

3.3.1 The Board will respond to incidents involving the inappropriate use of technology resources in a manner that is fair, proportionate, and appropriate to the circumstances.

3.3.2 In determining the appropriate response, the Board may consider factors including but not limited to:

i) the nature and severity of the incident;

ii) whether the conduct was intentional or accidental;

iii) the impact on students, staff, Board operations, or Board technology resources;

iv) previous incidents involving the individual;

v) applicable legislation, Board policies, administrative procedures, and collective agreements.

3.3.3 Corrective or disciplinary measures may include, but are not limited to, the following:

Students

i) Restriction, suspension, or loss of access to Board technology resources.

ii) Parent/guardian notification.

iii) Restorative practices, counselling, or digital citizenship learning opportunities.

iv) Restitution for the loss of or damage to Board-owned technology resources, where appropriate.

v) Disciplinary action in accordance with the *Education Act*, NCDSB policies, and the school's Code of Conduct;

vi) Referral to law enforcement where appropriate.

Staff

i) Coaching, education, or additional training.
ii) Restriction or suspension of access to Board technology resources.
iii) Restitution for the loss or of damage to Board-owned technology resources, where appropriate.
iv) Corrective or disciplinary action in accordance with NCDSB policies, applicable legislation, employment agreements, and collective agreements.
v) Referral to law enforcement where appropriate.

Other Authorized Users

Where concerns involve an Other Authorized User (including parents/guardians, volunteers, contractors, visitors, or other authorized individuals), the Board may take one or more of the following actions, as appropriate:

i) Restrict, suspend, or revoke access to Board technology resources, systems, or facilities.
ii) Require restitution for the loss of or damage to Board-owned technology resources, where appropriate.
iii) Report the matter to the individual's employer, sponsoring organization, or supervising authority, where applicable.
iv) Terminate volunteer, contractor, or visitor access privileges.
v) Refer the matter to law enforcement or other authorities where appropriate.

Trustees

Where concerns involve a Trustee, the matter will be addressed in accordance with the *Education Act*, the Trustee Code of Conduct, NCDSB policies, and other applicable governance requirements.

i) Education or guidance regarding the appropriate use of Board technology resources.
ii) Restriction of access to Board technology resources, where appropriate.
iii) Restitution for the loss of or damage to Board-owned technology resources, where appropriate.
iv) Measures available under the Trustee Code of Conduct or applicable legislation.
v) Refer to the matter to law enforcement or other authorities where appropriate.

3.4 Privacy and Cybersecurity Incidents

3.4.1 Suspected privacy breaches, cybersecurity incidents, unauthorized disclosure of personal information, or compromise of Board technology resources shall

be reported immediately to the ICT Department and the appropriate Supervisory Officer.

3.4.2 The Board will respond to such incidents in accordance with applicable legislation, Board policies, cybersecurity best practices, and any applicable reporting obligations.

3.4.3 Where appropriate, the Board will take reasonable steps to contain the incident, assess its impact, notify affected individuals or authorities as required, and implement measures to reduce the risk of future occurrences.

4.0 DIGITAL CITIZENSHIP & RESPONSIBLE INNOVATION

The Northeastern Catholic District School Board is committed to fostering a culture of safe, ethical, responsible, and effective technology use. Through ongoing education and professional learning, the Board will support students, staff, and other members of the school community in developing the knowledge, skills, and judgment necessary to use technology responsibly and in ways that reflect Catholic values.

The Board will promote learning opportunities that include, but are not limited to:

i) Safe, ethical, and responsible use of technology and digital resources.
ii) Digital citizenship, including respectful online communication, responsible participation in digital communities, and the prevention of cyberbullying and online harassment.
iii) Cybersecurity awareness, including password security, phishing awareness, and the protection of Board systems and information.
iv) Privacy, confidentiality, and the responsible collection, use, storage, and sharing of personal information in accordance with applicable legislation.
v) The appropriate, ethical, and responsible use of artificial intelligence (AI) tools, including understanding their capabilities, limitations, potential biases, privacy implications, and the importance of maintaining academic integrity and professional responsibility.
vi) Critical thinking, digital literacy, and information evaluation to support informed and responsible decision-making in an evolving digital environment.
vii) Catholic teachings and values that promote respect for the dignity of every person, responsible stewardship of technology, truthfulness, integrity, and care for the common good in digital spaces.

5.0 MOBILE COMMUNICATION DEVICES

5.1 The Board may provide mobile communication devices or authorize the use of personal devices where operationally required to support Board business.

5.2 Board-issued mobile devices are intended to support timely communication, operational continuity, and emergency response where required.

5.3 Based on operational requirements, the Chief Executive Officer or designate, determines which positions are eligible for:

i) a Board-issued mobile device;
ii) Reimbursement for an authorized personal device;
iii) Other mobile communication arrangements.

5.4 Uses of Board-issued devices are expected to:

i) use the device primarily for Board business;
ii) protect the device from loss, theft, or unauthorized access;
iii) comply with Board cybersecurity requirements;
iv) promptly report loss, theft, or compromise;
v) return the device upon request or when employment or eligibility ends.

5.5 Where personal devices are authorized for Board business, users shall:

i) comply with all Board privacy and security requirements;
ii) use approved Board applications where required;
iii) understand that Board information created or stored on personal devices remains subject to applicable legislation, including MFIPPA;
iv) cooperate with security measures necessary to protect Board information.

5.6 To ensure the privacy and security, users shall:

i) use strong authentication;
ii) maintain current operating system updates;
iii) not share devices used for Board business without appropriate safeguards;
iv) immediately report suspected privacy breaches or cybersecurity incidents.

5.7 The Board may provide mobile communication devices or reimburse authorized mobile communication expenses where operationally appropriate. Reimbursement and cost management shall be administered in accordance with this procedure.

i) Reimbursement amounts shall be established annually through the Board's budget process and approved by the Chief Executive Officer.
ii) Users are responsible for personal charges incurred on Board-issued devices unless otherwise authorized.
iii) International roaming or other exceptional charges require prior approval.

5.8 Technical support will be provided for Board-issued mobile communication devices. Support for personally owned devices is limited to assisting users with access to Board-approved systems and services.

5.9 Lost, stolen, or replaced devices shall be immediately reported. The Board may remotely disable or erase Board information where appropriate.

6.0 RELATED FORMS AND DOCUMENTS

Annual acknowledgement will be completed electronically.

Chief Executive Officer: *Tricia Stefanic Weltz*
Date: September 2026