Waterloo Catholic District School Board
Quality, Inclusive, Faith Based Education

Administrative Procedures Memorandum APS017

Responsible Use of Information Technology and Electronic Data - Staff

Date of Issue:	September 2003
Reviewed/Revised:	February 2006, March 2012, December 2012, May 2013, September 2014, May 2015, September 2016, October 2016, October 2017, December 2020, January 2022, March 2024, September 2024, March 2025
Memo To:	All Stakeholders
From:	Director of Education

ACCESSIBILITY:
To request this file in large print, please email aoda@wcdsb.ca or call (519) 578-3660.

PURPOSE:

The intent of this Administrative Procedures Memo is to provide direction to staff using Waterloo Catholic District School Board (WCDSB) information technology assets and resources.

The Waterloo Catholic District School Board supports the benefits that technology can bring to enable its daily operating activities and student achievement. All users are required to know, acknowledge they have read, and abide by this policy to ensure information technology resources are being used in a safe and responsible manner.
.

REFERENCES:

- Ontario Education Act
- APS012: Mobile and Personal Technology
- APS024: Workplace Harassment/Discrimination Prevention
- APS035: Electronic Mail and Social Media Use Guidelines
- APC016: Records Information Management
- APC018: Code of Conduct
- APC040: Privacy Breach Protocol
- APC052: Responsible Use of Information Technology and Electronic Data - Student
- Policy/Program Memorandum 128
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Personal Health Information Protection of Privacy Act (PHIPA)
- Children, Youth, and Family Services Act (CYFSA)
- Ontario College of Teachers Professional Advisories
- Regulated Professions' Codes of Conduct and Professional Standards (Social Workers, Speech and Language Pathologists, Audiologists, Psychologists)
- Ontario Catholic School Graduate Expectations
- ECNO VASP (Vetting of Application Security and Privacy) https://ecno.org/projects/vasp/

- Canadian Anti-SPAM Legislation.
- Approved Apps List available through Privacy, Records, and Information Management Staff Portal site

FORMS:

- APS017-08F: Virtual Private Network (VPN) User Agreement (Online form to be completed by supervisor)
- APS017-09F: Staff Device Borrowing Form (Online Form)

REPORTS:

- N/A

APPENDICES:

- Appendix A: Guest Wireless Network Terms and Conditions/Acceptable Use Agreement
- Appendix B: Responsible Use of Technology & Electronic Data Access, WCDSB Employees & Trustees Consent

COMMENTS AND GUIDELINES:

Definition

Information technology resources are used to create and provide an environment that enables the delivery of education to students and the tools needed to administer the business of the Board. IT resources are both physical and virtual. Physical resources include, for example, computers, computing hardware, peripherals, printers and scanners, learning devices, and any item that supports the Board's ability to deliver education.

Information assets are any data, information, documents, or records that are collected or created by WCDSB for the purposes of delivering education or administering the Education Act. Board information assets must be managed and safeguarded in the same way as devices or other assets are. Information assets include, but are not limited to, records, student personal information, plans, reports, confidential records, software, applications, third party subscriptions or services, or websites that are used to support the delivery of education.

With few exceptions, information assets are disposed of at the end of the information lifecycle according to records retention schedules.

Consent Forms

All staff and trustees accessing WCDSB information or information technology assets or resources must agree to abide by Responsible Use conditions.

1. **WCDSB Employees and Trustees** - Must acknowledge their consent as outlined in the Responsible Use of Technology & Electronic Data Access, WCDSB Employees & Trustees Consent (APS017-BX: Appendix B).

   Only the Manager/Supervisor can request the WCDSB Virtual Private Network connection on this form: Virtual Private Network (VPN) User Agreement (Form APS017-08F).

2. All **Students, Staff and Visitors** are subject to the regulations outlined in the Guest Wireless Network Terms and Conditions/Acceptable Use Agreement (APS017-AX: Appendix A).

Responsibilities

WCDSB is committed to leveraging digital tools in the service of student learning.

All Users agree to respect intellectual property rights, copyright, privacy rights, anti-defamation, and criminal laws. Users also agree to respect Catholic values, Safe Schools guidelines, including anti-bullying and anti-harassment policies of WCDSB.

Requirements

- Information and information technology assets and resources must only be used in an ethical manner consistent with the educational and work-related purposes for which they are provided.
- Users must protect assets and resources, e.g., by using passwords on devices and accounts, and by applying safeguards appropriate to the sensitivity of the asset. Users are responsible for the repair and replacement of damaged devices used on board property and home use, and for excessive overage usage of Board provided services (e.g., Wi-Fi hot spots); the Board reserves the right to determine what a data use overage entails.
- Staff must complete training annually on Privacy and Cybersecurity

Conditions

TABLE OF CONTENTS:

1. Acceptable Use of Technology
2. Prohibited Activities
3. Electronic Computing Equipment Borrowed or Assigned to Staff
4. Approved, Restricted, and Prohibited Digital Tools and Resources
   a. Definition
   b. Approved Tools and Resources
   c. Restricted and Prohibited Tools and Resources
   d. Procedure for Requesting Applications and Web Tools
   e. Application Review Process
   f. Consent from Parent/Guardian
5. Understanding Privacy Considerations
6. Parent-Teacher Electronic Collaboration and Communication
7. E-Mail Based Tools
8. Verifying Parental Access and Custodial Rights
9. Monitoring, Access, and Enforcement
   a. Definition
   b. Duties
   c. Privileges
   d. Investigations
10. Working from Home / Working Remotely
11. Incident Reporting
12. Information Security and Privacy Training

1. Acceptable Use of Technology

- Employees will promote the ethical use of technology resources and will provide guidance, support, supervision, and instruction to students as they access educational resources.

- Employees must be aware that the work product(s) they create for board purposes using WCDSB technology and on WCDSB-managed systems remain the property of WCDSB.
- All WCDSB technology supplied to or used by employees, trustees, students, or volunteers remains the property of the WCDSB.
- WCDSB has the right to monitor all activity on its technology and systems and is responsible for ensuring its information assets and information technology network and resources are secure and functioning properly. Staff may from time to time, on a need-to-know basis, access content created by users for the purposes of troubleshooting, network management, or other investigations related to security, privacy, or policy compliance issues.
- WCDSB is responsible for ensuring the health and operational capacity of technology, equipment, systems, networks, and other information or information technology assets. WCDSB authorizes certain individuals to monitor and manage these assets. WCDSB will also conduct activity logging and auditing to ensure compliance with its responsibilities and obligations.
- All routers, network devices, or other Wi-Fi-enabled tools must be approved prior to being connected to the Board network.
- All users are responsible for exercising good judgement when accessing or using WCDSB information and information technology assets. WCDSB respects users' privacy rights, subject to the need to protect, investigate, repair, or prevent a breach, risk, or other threat to information or information technology assets.
- Accounts are not to be shared unless explicitly authorized by the Chief Information Officer or delegate.
- Authorized users are responsible for the security of their passwords and accounts.
- All users must secure computer and computing devices with a password-protected lock screen, which will be automatically activated after 10 minutes. To aid in the flow of classroom instruction, teachers and those who fall within the academic group are subject to an automatic lock screen timeout of 30 minutes. Users who are leaving computing devices unattended are responsible for ensuring the device is locked, logged out of, or turned off to prevent unauthorized access.
- Collections, uses, and disclosures of personal information must be done in accordance with the requirements of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) or Personal Health Information Protection Act (PHIPA) as appropriate; users must not post or upload personal information to the Internet without legal authorization or consent of the person affected.
- MFIPPA grants anyone a right to request information in the custody or control of WCDSB. Users are responsible for managing Board information assets and must provide support in response to a request for access to information using Freedom of Information laws.
- Use of WCDSB technology for individual commercial purposes or personal financial gain is prohibited.
- WCDSB assumes no liability for any direct or indirect damages arising from the user's connection to the Internet. WCDSB is not responsible for the accuracy of information found on the Internet and only facilitates access and dissemination of information through its systems. WCDSB is not responsible for management or support for personal devices.
- Only Board-approved Virtual Private Network (VPN) tools are permitted to connect to Board-managed resources.
- In those cases where students require assistance from educators to log in or otherwise access WCDSB-assigned devices, educators will need to ensure all accounts have been logged out of.

2. Prohibited Activities

- Posting student work, photographs and/or video images on any public website without prior written consent from the student's parent or guardian, except where noted in the Student Personal Information Collection / Use / Disclosure Notice (APC023-AX: Appendix A).
- Posting student's personal information such as birthdays, class lists, marks and demographic information.

- Copying, downloading, or using copyrighted and/or intellectual property materials such as text, music, or images in excess of permitted fair dealing and without authorization from the rights holder.
- Using the internet excessively during the school or workday for purposes unrelated to learning or work.
- Accessing content that is illegal, harassing, obscene, pornographic, racist, libelous, threatening, promoting physical violence, or sexually explicit.
- Using electronic mail to send obscene, threatening, harassing, libelous, discriminatory, or inflammatory messages.
- Installing unauthorized software.
- Connecting to the WCDSB network non-Board devices (e.g., routers, Wi-Fi devices, Google Home), or devices that are not issued by WCDSB.
- Causing disruption of the Internet and/or Intranet.
- Using WCDSB technology at any location for the purposes of bullying and/or harassing.
- Damaging the work of an individual or organization.
- Using inappropriate language or being disrespectful when communicating over the Internet.
- Accessing, collecting, using, or disclosing private or personal information without prior authorization.
- Using the internet or email accounts in a manner that is not consistent with the mission of WCDSB, misrepresents WCDSB, or violates any of WCDSB's policies and procedures.

3. Electronic Computing Equipment Borrowed or Assigned to Staff

- Staff will often be assigned laptops, Chromebooks, tablets, iPads and other electronic computing equipment. Schools will also have sets of computing devices such as laptops, Chromebooks, tablets, or web cameras. These devices can be taken home to work on job-related tasks and projects overnight, on weekends or for educational and work-related events with the consent of the employee's supervisor.
- If equipment is damaged or lost through employee negligence, employees will be required to reimburse the WCDSB for the equipment replacement cost. The WCDSB will issue an invoice to the employee for the replacement cost and the employee will have the choice of one of the following reimbursement plans:
    a. Employee to pay the entire balance of the invoice at time of receipt, or
    b. Payroll deduction over a period no longer than three months
- Upon termination of the employment relationship with WCDSB employees will surrender all information and information technology assets supplied by the Board, including but not limited to information about work, students, or other any other confidential nature.
- Former employees are not permitted to access external services or applications using a board-managed account (e.g., first name. last name [at] wcdsb.ca) after the employment relationship has concluded. Exceptions may be granted by the Director.
- Employees are responsible for the set-up of equipment off site. Information Technology Services will provide remote support for WCDSB assets and resources during office hours. Employees must open a ticket using the IT Helpdesk to request support.
- Employees who require IT support when on-site at WCDSB locations can open a ticket through the IT Helpdesk.

4. Approved, Restricted, and Prohibited Digital Tools and Resources

a. Definition

WCDSB uses a range of tools, services, and environments to support its information technology network, resources, and assets. Many of the services WCDSB uses are contracted out to third party service providers. Some services are simple and single use, for example an application that supports learning math; other services are complex and have many sub-services, such as Office365, the Google Suite for Education products, Brightspace by D2L, or Aspen, the student information system.

Digital Tools and Resources include stand-alone applications ('apps'), websites, or other dedicated sites or services.

Apps and digital tools are reviewed and approved or rejected using the following categories:

- **Green** (safe and approved for use in WCDSB) [APPROVED]
  - This is approved, meaning it has been assessed and determined to be safe to use.
- **Yellow** (approved, but with conditions and usage notes) [RESTRICTED]
  - This is approved, but has conditions restricting use.
- **Blue** (approved for Special Education, or under a SEA claim) [RESTRICTED]
  - This is approved but is restricted to use with specific groups and is not approved for other uses.
- **Red** (not approved; not safe for use) [PROHIBITED]
  - This is prohibited, meaning the app has either not been assessed, or it has been assessed and determined to present a significant risk or danger.

b. Approved Tools and Resources

Apps, tools, and resources that are safe to use are considered 'green', 'yellow', or 'blue' because they have gone through a review process to confirm that they are appropriate and safe for use in WCDSB. There are four review categories:

- Pedagogy
- Purchasing
- Information Technology (integration, security), and
- Privacy and Records Management

Once the reviews are completed and if approval is granted the app or digital resource will be added to the Approved Apps list.

Approvals may be revoked at any time subject to further assessment.

The Approved Apps list is accessible here:

- Internal to WCDSB:
  - https://wcdsbca.sharepoint.com/ithelpdesk/prim/Lists/Applist_REV_20211208_3/Simplified.aspx
- Public / External to WCDSB:
  - https://www.wcdsb.ca/about-us/policies-and-administrative-procedures/responsible-use-of-information-technology-and-electronic-data-aps017/

c. Restricted and Prohibited Tools and Resources

The review and approvals process results in the determination of approved, restricted or prohibited status.

- **Restricted** means that the app is approved with conditions and its use is subject to further review. There are times when an app will be approved for some uses (e.g., Special Education) but is not approved for other, more general uses. **Consent forms do not automatically change the restricted status of an app.**

- **Prohibited** means that the app, digital tool, or resource is not approved and must not be used under any circumstances, regardless of whether consent is obtained or not.

d. Procedure for Requesting Applications and Web Tools

Any app, digital tool, or resource must be reviewed before it is approved for use in WCDSB.

Requests for apps and digital tools can be for a NEW app, or to DEPLOY and existing app. Requests must be submitted through a **Helpdesk** ticket to engage the app review process.

e. Application Review Process

1. Requester completes Helpdesk ticket requesting NEW app. If request is to DEPLOY an existing app that has already been approved the following steps are not required.
   - **Academic:** Program Department to recommend application with determination that requested resource 1) has pedagogical value, and 2) existing approved apps do not already have similar functionality 3) Check ECNO VASP privacy evaluation score shows a low identified risk.
   - **Administrative:** SBO approval with business case.
   - **Special Education**: Assistive technology requests follow a separate process defined by urgency and special circumstances related to accommodation and equity.
2. Budget approval if required, through APS015 process with Procurement approval.
3. IT evaluates implementation impact on current systems.
4. Privacy Officer will assess privacy impact, document assessment, and provide advice or notes for safe use of resource as required.
5. Superintendent final approval of application if needed.
6. App Review Team records approved status in WCDSB Approved Apps List.

f. Consent from Parent/Guardian

There are times when consent to use a tool may be required from parents/guardians. Consent may be required for several reasons, including:

- The vendor specifically states that written consent is required (e.g., for students under 13 years of age).
- The digital tool or app is not on the approved apps list but is being used for a specific reason subject to conditional approval.

Consent must be documented using the Third Party Online Tools/Applications, Parent/Guardian Consent (Form APC052-04F).

The legal age for consent in Ontario is 18 years old.

Consent cannot be used to make a prohibited app approved. Although consent may be used to authorize use of an app that is not on the approved apps list, for example in a time-limited way or for special events, there may be times when these apps are blocked entirely or removed from use in the WCDSB network environment. Administrators, teachers, or others who need help with the status of App Approvals should submit a Helpdesk ticket requesting a review.

Any use of restricted sites and apps must be done following strict data minimization and de-personalization practices. Student personal identifiers such as names, barcodes, or other identifiers must be limited and removed from the application or tool once the work or activity is completed.

Consent forms are retained at the school. Except for time-limited or special circumstances, consent is deemed to be granted annually for each school year.

Parents/guardians can withdraw consent at any time by providing notice in writing to the school. Parents/guardians should notify a student's teacher that consent has been withdrawn. In certain circumstances students have the capacity to consent on their own behalf.

5. Understanding Privacy Considerations

For a more information on understanding School Board and Contracted tools (Approved/Green) and External tools (Restricted/Red; Prohibited).

Welcome To Privacy and Records Information Management - Home (sharepoint.com)

6. Parent – Teacher Electronic Collaboration and Communication

Communication and collaboration between teachers and parents is enabled by many online tools; staff may wish to use these tools to increase parent engagement. Some of these tools are approved and part of the WCDSB environment, which means that they have been vetted and contracted through WCDSB or the Ministry of Education and have specific security and privacy agreements in place. Examples include:

- D2L Parent Portal
- D2L Notifications Pulse App
- Aspen Parent Portal
- School Cash Online
- School Messenger

Tools not contracted by WCDSB or the Ministry of Education and that do not have security and privacy agreements in place are restricted or prohibited.

7. E-Mail Based Tools

The Canadian Anti-SPAM Legislation applies to any parent or general public email-based communication. Recipients of the e-mail must give explicit consent to receive the messaging and they must be able to easily unsubscribe from it. See APS035 for Electronic Mail and Social Media Use Guidelines.

8. Verifying Parental Access and Custodial Rights

Any educator communicating with parents/guardians must first confirm the current contact information using the parent contact details in the student's Aspen profile, which is the authoritative source for student information in WCDSB. If this information is out of date or inaccurate it is the responsibility of the parent/guardian to update using the student verification process.

9. Monitoring, Access, and Enforcement

a. DEFINITION

The System is provisioned by the Board for work and educational purposes that give it a strong interest in having access to accounts and information. The Board may access accounts and information for its legitimate purposes, which includes:

- Perform System maintenance and repair
- Investigating System misuse
- Proactively monitoring and auditing for System misuse
- Complying with legal obligation

- Supporting work continuity
- Conducting research

Personal use of the System is a privilege. For personal activities use a personal device that is not connected to the System. A password allows us to identify how you are using the System and does not preclude the Board from accessing System data.

b. DUTIES

- Duty to report Internet Address

  If a person is advised, in the course of providing an Internet service to the public, of an Internet Protocol (IP) address or a Uniform Resource Locator (URL) where Child Sexual Abuse Material (CSAM) may be available to the public, the person must report that address or Uniform Resource Locator to the organization designated by the regulations, as soon as feasible and in accordance with the regulations.

- Duty to notify police officer

  If a person who provides an Internet service to the public has reasonable grounds to believe that their Internet service is being or has been used to commit an offence concerning CSAM, the person must notify an officer, constable or other person employed for the preservation and maintenance of the public peace of the fact, as soon as feasible and in accordance with the regulations.

c. PRIVILEGES

- All users are expected to comply with this procedure. Failure to comply with this procedure will result in disciplinary action including but not limited to loss of access to information and information technology assets, tools, and resources. Student violation of this procedure will be dealt with in accordance with applicable WCDSB policies and procedures.
- If an employee violates this procedure, the employee will be provided with notice of such violation. An employee's access to WCDSB's electronic network may be denied, restricted, or suspended and additional action may be taken up to and including dismissal.
- Appropriate legal authorities will be contacted if there is any suspicion of illegal activity.

d. INVESTIGATIONS

- Upon a reasonable suspicion of illegal activity or activity that contravenes the duties, privileges, or requirements of Board policies, an investigation may be initiated to determine the scope and related facts.
- Investigations involving user accounts will be managed through the IT department according to case files.
- Investigations will be conducted by specific, named, and approved individuals further to demonstrable need and severity. Access to investigation information will be limited to least privilege and will be retained according to Board policy.
- In certain cases, WCDSB may disclose information to the police under MFIPPA s.32(g).

10. Working From Home / Working Remotely

- Any work that takes place away from the main work environment (e.g., school or office) must continue to practice safe data hygiene and ensure proper safeguards are applied to WCDSB information and information technology assets.
- For additional details on managing student personal information when using WCDSB tools and resources, please see Student Personal Information Collection/Use/Disclosure – APC023

11. Incident Reporting

If a suspected breach or compromise is suspected, a ticket should be immediately logged via emailing the IT Helpdesk (helpdesk@wcdsb.ca) and fully describe the incident.

Suspected data breaches or compromises should be not resolved without the assistance of IT staff. Doing so may result in further risk and exposure on the WCDSB network. IT will triage the suspected incident according to criticality and advise of next step. Do not forward any suspicious communication.

12. Information Security and Privacy Training

All employees are required to complete information security and privacy training upon hire at WCDSB or as required by the Board during the course of employment.