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

Administrative Procedures Memorandum #APC052

Responsible Use of Information Technology and Electronic Data - Student

Date of Issue: January 2022
Reviewed/Revised: March 2024, August 2024

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 anyone using Waterloo Catholic District School Board (WCDSB) information technology assets and resources. The focus audience of this Administrative Procedure is students and parents.

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 (IT) resources are being used in a safe and responsible manner.

REFERENCES:

- Ontario Education Act
- APC016: Records Information Management
- APS035: Electronic Mail and Social Media Use Guidelines
- APS012: Mobile and Personal Technology
- APS017: Responsible Use of Information Technology and Electronic Data - Staff
- APC018: Code of Conduct
- 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)
- Regulated Professions' Codes of Conduct and Professional Standards (Social Workers, Speech and Language Pathologists, Audiologists, Psychologists)
- 21st Century Shepherds: Stewards of Student Data- CCC
- Ontario Catholic School Graduate Expectations
- ECNO VASP (Vetting of Application Security and Privacy) https://ecno.org/projects/vasp/
- Canadian Anti-SPAM Legislation.
- WCDSB Staff Cybersecurity Training

- Approved Apps List available through Privacy, Records, and Information Management Staff Portal site
- Child in Need of Protection (APS020-01F_SuspectedChildProtectionReportRecordExtended.pdf (wcdsb.ca)

FORMS:

- APC052-01F: Responsible Use of Technology & Electronic Data Access, Students Grades JK to 3 Consent
- APC052-02F: Responsible Use of Technology & Electronic Data Access, Students Grades 4 to 8 Consent
- APC052-03F: Responsible Use of Technology & Electronic Data Access, Students Grades 9 to 12 Consent
- APC052-04F: Third Party Online Tools/Applications, Parent/Guardian Consent
- APC052-06F: SEA Equipment, Request & Take Home Consent (Online Form)
- APC052-07F: Esports Information & Consent (Online Form)
- APC052-08F: Esports Information & Consent (Print Form)

REPORTS:

- N/A

APPENDICES:

- Appendix A: Guest Wireless Network Terms and Conditions/Acceptable Use Agreement (APS017-AX)

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 that 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.

Personal Mobile Devices: Includes smartphones, tablets, and any other electronic devices used for communication or accessing digital content. A mobile device is any personal electronic device that can be used to communicate or access the internet, such as a laptop, cellphone, tablet or smart watch.

Social Media Platforms: Online platforms where users create and share content or participate in social networking (e.g. Snapchat, Instagram, X …).

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

Consent Forms

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

1. **Students** - Consent forms are specific to each grade category and must be signed annually:
    - JK-Grade 3 (Form APC052-01F)
    - Grades 4-8 (Form APC052-02F)

- Grades 9-12 (Form APC052-03F)

2. **Parents** – Consent forms are required when using certain applications or accessing certain web sites. Teachers will distribute the Third Party Online Tools/Applications Parent/Guardian Consent (Form APC052-04F) when required.

3. 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.

The responsibilities outlined in this policy apply to every use of an account issued by WCDSB regardless of whether the account is accessed by a student in a classroom, remotely, or on a personal device. A parent logging in with a child's account (e.g., to assist with homework) must still conduct themselves according to the guidelines that apply to the child's use of the account.

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. Wifi hot spots); the Board reserves the right to determine what a data use overage entails.

Conditions

TABLE OF CONTENTS:

1. Acceptable Use of Technology
2. Prohibited Activities
3. Approved, Restricted, and Prohibited Digital Tools and Resources
   a. Definition
   b. Restricted and Prohibited Tools and Resources
   c. Consent from Parent/Guardian
4. Parent-Teacher Electronic Collaboration and Communication
5. Verifying Parental Access and Custodial Rights
6. Bring Your Own Personal Mobile Device
7. Monitoring, Access and Enforcement
   a. Definition
   b. Duties
   c. Privileges
   d. Investigations

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.
- 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.
- All users must keep passwords secure. 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 must be automatically activated after 10 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.

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, or school sanctioned esports play.
- Accessing content that is illegal, harassing, obscene, pornographic, racist, libelous, threatening, promoting physical violence, or sexually explicit.
- Using electronic mail, chat, or other messaging tool 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. An acceptable exception is within a school sanctioned esports event where personal gaming consoles or portable gaming devices could be connected.
- 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.
- While at school there is significant filtering and safeguarding related to student access to particular websites and resources. At home parents may want to add school accounts to a safeguarding service of their choice. WCDSB does not endorse or recommend any particular parental control product as some may or may not work with WCDSB accounts. Instead, WCDSB recommends contacting your internet service provider and/or checking router settings for parental control options.
- Social media platforms can only be used by students at school for educational purposes, directed by an educator. Requests for exceptions must be submitted through the IT Helpdesk for approval.

3. 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, 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 subject to the process outlined in APS017.

The Approved Apps list is accessible here:

- Public / External to WCDSB:
  - https://www.wcdsb.ca/about-us/policies-and-administrative-procedures/responsible-use-of-information-technology-and-electronic-data-aps017/

b. 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.

c. 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.

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.

4. 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/Safe Arrival

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.

5. 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.

6. Bring Your Own Personal Mobile Device

- Be aware that the Waterloo Catholic District School Board (WCDSB) is not liable for any complications arising at any of its locations, including failure of the device or any software installed thereon.
- The Waterloo Catholic District School Board cannot provide any technical support for personal mobile devices or personal accounts.
- It is your responsibility to contact the vendor or your local computer repair service directly, should you require technical assistance or support of any kind.
- Users who bring their own personal mobile devices are expected to take reasonable efforts to prevent introducing viruses or other malware to the WCDSB infrastructure.
- Personal Mobile Devices are forbidden to be used in the classroom without the educator's expressed permission. See APS018: Code of Conduct
- Students are responsible for their personal mobile device, how they use it and the consequences of not following the school board's policy.
- using personal mobile devices during instructional time except for under the following circumstances: for educational purposes, as directed by and educator, for health and medical purposes as reflected in the student's plan of care, or to support special education needs as reflected in the student programming (eg, IEP)

- Educators will monitor the use of personal mobile devices.

- Questions regarding the collection and use of this information should be directed to the School Principal.

7. 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:

- Performing System maintenance and repair
- Investigating System misuse
- Investigating security or privacy incidents or breaches
- 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 containing 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.

- Duty to report a child in need of protection

  Any person who believes they see or know of a child in need of protection must report to a teacher, educator, administrator, or directly to the local Family and Children's Services.

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.
- 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).
- Practices and disciplinary action following investigations will follow Board policy APC018 – Code of Conduct