Waterloo Catholic District School Board

Administrative Procedures Memorandum

#: APS017

Responsible Use of Information Technology and Electronic Data

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
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 resources.

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

REFERENCES:

- Municipal Freedom of Information and Protection of Privacy Act
- Mission and Vision of the WCDSB
- WCDSB Harassment and Discrimination Policy
- Ontario College of Teachers Professional Advisory
- Ethical and Responsible Use Of Information and Communication Technology - CCC
- WCDSB Code of Conduct
- Ontario Catholic School Graduate Expectations
- APS035: Electronic Mail and Social Media Use Guidelines
- Introduction to Privacy Video
- Password Management Video
- Understanding Privacy Considerations Video
- Canadian Anti-SPAM Legislation.

FORMS:

- APS017-01F: Responsible Use of Technology & Electronic Data Access, Students Grades JK to 3 Consent
- APS017-02F: Responsible Use of Technology & Electronic Data Access, Students Grades 4 to 8 Consent
- APS017-03F: Responsible Use of Technology & Electronic Data Access, Students Grades 9 to 12 Consent
- APS017-04F: Responsible Use of Outside Technology Equipment, Student Personal Electronic Device Consent
- APS017-06F: Third Party Online Tools/Applications, Parent/Guardian Consent

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
- Appendix C: Guidelines For Using Online Educational Tools (Third Party Apps)

COMMENTS AND GUIDELINES:

Definition

Information technology resources include but are not limited to the Internet, StaffNet, online learning environment (e.g. Class Net, Learning Management System), social networks (e.g. Facebook, Twitter), WCDSB-managed cloud environments (e.g. Google Apps for Education, Office 365, Desire 2 Learn), WCDSB-owned technology, and personal devices accessing WCDSB resources.

Consent Forms

1. **Students** - Prior to being granted access to information technology resources, all users are responsible for knowing and abiding by this policy and, signing an applicable Responsible Use Consent Form. Based on the student's grade, the following Consent forms will be used:

   - JK-Grade 3 (APS017-01F)
   - Grades 4-8 (APS017-02F)
   - Grades 9-12 (APS017-03F)

   Where students are using their own personal devices, the Responsible Use of Outside Technology Equipment, Student Personal Electronic Device Consent (Form APS017-04F) must be completed.

2. **Parents** – In certain circumstances, e.g. student use of a Red Site (described below), it may be necessary to request that parents complete the Third Party Online Tools/Applications Parent/Guardian Consent (Form APS017-06F).

3. **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).

4. **Students, Staff and Visitors** – must be aware of the regulations outlined in the Guest Wireless Network Terms and Conditions/Acceptable Use Agreement (APS017-AX: Appendix A).

Responsibilities

All Users must fully respect intellectual property rights including copyright, privacy rights, human rights (including the right of freedom from harassment), defamation, and criminal laws. In addition, users must fully respect Family Life Protocols, Safe Schools guidelines, as well as all other pertinent legislation, regulations, polices and guidelines in force.

The WCDSB is committed to providing all users with access to information technology resources and believes that this access will enhance opportunities for developing lifelong skills as independent learners, creative thinkers, enthusiastic problem solvers and effective communicators.

The WCDSB acknowledges that it is necessary to teach students critical thinking skills to make moral as well as intellectual decisions about the information and technology that they encounter.

The WCDSB accepts its responsibility to define “responsible use” of its information technology resources.

All users are responsible for:

- Ensuring that they use information technology resources in an appropriate manner in accordance with WCDSB policies, procedures and pertinent legislation.
- Using the WCDSB’s information technology resources in a responsible and ethical manner consistent with the educational, informational, and work-related purposes for which they are provided.
- Ensuring that any use of personal and WCDSB-issued technology devices that access WCDSB resources (e-mail, enterprise systems, student/staff data and information, social media etc.) are password protected.
- Ensuring that WCDSB-issued devices are used in accordance with the Highway Traffic Act and all applicable laws and legislation (e.g. it is illegal to handle a smartphone while driving).

Responsible Use - Terms and Conditions

1. All users of WCDSB information technology resources are responsible for appropriate and ethical behaviour at all times.
2. Employees will promote the ethical use of technology resources and will provide guidance, support, supervision, and instruction to students as they access educational resources.
3. Employees must be aware that the data they create with WCDSB technology and on WCDSB-managed systems remains the property of the WCDSB.
4. All users must be aware that the WCDSB cannot guarantee the confidentiality of information stored on any network or technology device belonging to the WCDSB because of the need to protect the WCDSB’s information and network.
5. All WCDSB technology supplied to, or used by, WCDSB employees, trustees, students and volunteers remains the property of the WCDSB which gives the WCDSB the right to monitor any and all activity on its technology and systems.
6. Users are responsible for exercising good judgement regarding the reasonableness of personal use. Users must not have any expectation of privacy when storing personal information on WCDSB networks or WCDSB-owned technology.
7. For security and network maintenance purposes, authorized individuals within the WCDSB may monitor technology, equipment, systems and network traffic at any time. The WCDSB reserves the right to audit technology, networks and systems on a periodic basis to ensure compliance with this policy.
8. All users must keep passwords secure and not share accounts. Authorized users are responsible for the security of their passwords and accounts.
9. All WCDSB-owned technology must be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or by logging off when the technology will be unattended.
10. Ensure that any information posted to the Internet is consistent with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).
11. Under MFIPPA, all electronic records are subject to a Freedom of Information request.

12. At no time will WCDSB technology be used for individual commercial purposes or personal financial gain. The WCDSB retains ownership, control and copyright over anything created, composed or otherwise developed using WCDSB technology resources.
13. The WCDSB assumes no liability for any direct or indirect damages arising from the user's connection to the internet. The WCDSB is not responsible for the accuracy of information found on the internet and only facilitates access and dissemination of information through its systems.

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 and tablets. 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:
  - Employee to pay the entire balance of the invoice at time of receipt
  - Payroll deduction over a period no longer than three months
- In the event that an employee terminates employment with the WCDSB, or his/her employment is terminated by the WCDSB, the employee will return the equipment on his/her last day.
- The employee is responsible for the set-up of equipment off site. Information Technology Services will provide hardware and software support in the WCDSB Office during regular office hours. Please note that Information Technology Services will not provide off site support at any time.

Cloud Computing (Green and Red Environments)

Cloud computing is the expansion and migration of local services and systems into a system of services that includes high capacity computing resources, storage in data farms, a range of computer applications, and opportunities for collaboration and connections. Many of the WCDSB's online services are now in contracted cloud computing environments. The three types of services associated with cloud computing are:

1. Single function end-user services such as Hotmail, Gmail, OneDrive, and Dropbox
2. Networking infrastructure with no end-user services, but rather the platform upon which the WCDSB builds its own Cloud-based applications and services (e.g., Microsoft Azure)
3. Hosted computing resources for the housing of WCDSB computer-based services not built by the WCDSB (e.g., Google Apps for Education, Desire 2 Learn, Office 365, eBase, Edge 4, Career Cruising, Synrevoice, Compass for Success, SmartFind Express, ERO, Power BI, etc.).

Green Sites

Green Sites are those sites that are under contract and managed by the Waterloo District Catholic School Board and/or the Ministry of Education. Inappropriate activities (such as cyber bullying) can be mitigated in a Green Site. Student information (including full student names and assessment data) is safe and secured in the appropriate systems. However, using a Green Site does not take away the onus to maintain personal levels of security over access to your materials and passwords. Green Sites include Google Apps for Education, Desire 2 Learn, Office 365, eBase, Edge 4, Career Cruising, Synrevoice, Compass for Success, SmartFind Express, ERO, and Power BI. For additional information on Green sites, refer to the Guidelines for Using Online Educational Tools (Third Party Apps) (APS017-CX: Appendix C).

Red Sites

Red Sites are those sites that are not monitored or under contract with the Waterloo Catholic District School Board and/or the Ministry of Education. Because Red Sites are privately owned and operated, the WCDSB cannot guarantee the same level of security as with a Green Site. Staff need to take further precautions when using Red Sites. Inappropriate activities (such as cyber bullying) are difficult to mitigate on a Red Site. For additional information on Red sites, refer to the Guidelines for Using Online Educational Tools (Third Party Apps)(APS017-CX: Appendix C).

Staff must note that care and consideration needs to be taken when inputting personal student information into a Red Site.

Parental consent may be required for student use of a Red Site. To seek parent consent, use the Third Party Online Tools/Applications, Parent/Guardian Consent (Form APS017-06F). As well, data stored in a Red Site would need to be depersonalized in some way (e.g. use initials rather than full names of students). Some examples of Red Sites are Dropbox, Prezi, WordPress, Edmodo, iCloud, Evernote or any sites not on the Green Site list above. While a site may say that 13 years of age is the age of consent of use for its product, the legal age of consent in Ontario for an agreement is 18 years of age.

Understanding Privacy Considerations Video

For a full understanding of Red and Green Sites, see Understanding Privacy Considerations video.

Parent – Teacher Electronic Collaboration and Communication

Tools providing for the communication and collaboration between teachers and parents have become available through many online tools. Many staff may wish to use these tools to increase parent engagement. Some of these tools are considered “Green” which means that they are WCDSB or Ministry of Education contracted with specific security and privacy agreements in place. These Green tools include:

- D2L Parent Portal
- Compass for Success Parent Portal
- Google Classroom Guardian

Tools not contracted by the WCDSB or the Ministry of Education do not have security and privacy agreements in place. An example of such a “Red” tool is Remind. These non-contracted tools can only be used if personal staff and student information is not communicated through the tool.

E-Mail Based Tools:

With any parent or general public e-mail based communication tool, Canadian Anti-SPAM Legislation must be adhered to. The recipient of the e-mail must give specific 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.

Parental Access and Custodial Rights:

Before initiating an invitation to participate in Google Guardian summaries, the classroom teacher needs to verify the parent/guardian email address using one of the following methods:

1. Consult the parent/guardian information section for the email address listed on the Student Information Verification Form that is generated from the student registration forms collected at the beginning of the year. The registration form indicates:
    - Personal information is collected on the WCDSB Online Registration site and/or on this form pursuant to the Education Act s265 and 266. Information will be used for communications, educational planning and to establish the Ontario Student Record (OSR). Please note that any email addresses provided may be used to send communication which may be commercial in nature. Any questions related to the collection, use, and disclosure of student information should be directed to the Principal.

2. The parent/guardian email address can also be verified by logging into the Compass for Success Dashboard and viewing the contact information in the student profile (access to student, guardian and access to records - by clicking on the CONTACTS tab above the photo of the student).

Responsible Use of WCDSB Technology

All users of WCDSB technology are prohibited from:

1. Posting student work, photographs and/or video images on any website without prior written consent from the student's parent or guardian.
2. Posting student's personal information such as class lists, marks and demographic information in a non-secured environment.
3. Copying or downloading copyrighted and/or intellectual property materials such as music and images.
4. Using the internet excessively during the school or workday for purposes unrelated to learning or work.
5. Accessing illegal, harassing, obscene, pornographic, racist, libellous, threatening, promoting physical violence or sexually explicit resources.
6. Using electronic mail to send obscene, threatening, harassing, libellous, discriminatory, or inflammatory messages.
7. Installing unauthorized software.
8. Causing disruption of the internet and/or intranet.
9. Using WCDSB technology at any location for the purposes of bullying and/or harassing.
10. Damaging the work of an individual or organization.
11. Using inappropriate language or being disrespectful when communicating over the internet.
12. Accessing private or personal information without prior authorization.
13. Using the internet or email accounts in a manner that is not consistent with the mission of the WCDSB, misrepresents the WCDSB, or violates any of the WCDSB's policies and procedures.

Privileges

- All users are expected to comply with this procedure. Failure to comply with this procedure will result in disciplinary action.
- In the event that an employee has violated this procedure, the employee will be provided with notice of such violation. An employee's access to the 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.
- Student violation of this procedure will be dealt with in accordance with WCDSB policy and procedures.