COMMISSION SCOLAIRE SIR-WILFRID-LAURIER
SIR WILFRID LAURIER SCHOOL BOARD

Policy nº 2000-IT-01:	Use of Information and Communication Technology Resources Policy

Approved:	Resolution nº	000322-IT-0179
Revised:	Resolution nº	CC-081022-CA-0032 CC-180523-IT-0123
Origin:	Information Technology	

Policy Outline:

NOTE: The masculine gender, when used in this document, refers to both women and men. No discrimination is intended.

A glossary of Terms

Access: To store data on and retrieve data from a disk or other peripheral device. (2) The entrance to the Internet or other online service or network. (3) In computer security, the opportunity for use of a resource.

Cloud services: Is a general term used to include a variety of computing and information services and applications run by users across the Internet (in the "Internet cloud") on the service provider's systems, instead of run "locally" on personal computers or campus-based servers. These Internet-based services are sometimes called "software as a service" (SaaS), or "platform as a service" (PaaS), or "hosted" applications, storage or computing.

Data: Data may refer to any electronic file no matter what the format: database data, text, images, audio and video. Everything read and written by the computer can be considered data except for instructions in a program that are executed (software).

E-mail: (Electronic-MAIL) The transmission of text messages and optional file attachments over a network.

File: A computer file is a block of arbitrary information, or resource for storing information, which is available to a computer program and is usually based on some kind of durable storage. A file is *durable* in the sense that it remains available for programs to use after the current program has finished.

Internet: The Internet is a worldwide, publicly accessible series of interconnected computer networks that transmit data using the standard Internet Protocol (IP). It is a "network of networks" that consists of millions of smaller domestic, academic, business, and government networks, which together carry various information and services, such as e-mail, online chat, file transfer (FTP), and the interlinked web pages and other resources of the World Wide Web (WWW).

Information Technology and Communication Technology (ICT) Resources: any technology equipment, including computers, peripherals, software, networking devices, IP networks (wired or wireless), IP phones, IP cameras, IP access control and IP intercoms.

IP Telephony: The two-way transmission of voice over a packet-switched IP network, which is part of the TCP/IP protocol suite. The terms "IP telephony" and "voice over IP" (VoIP) are synonymous. However, the term VoIP is widely used for the actual services offered while IP telephony often refers to the technology behind it. In addition, IP telephony is an umbrella term for all real time applications over IP, including voice over instant messaging (IM) and videoconferencing.

Malware: Is malicious software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Types of malware include viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware and adware.

Ransomware: Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to obtain a decryption key.

Network: A system that transmits any combination of voice, video and/or data between users. The network includes the network operating system in the client and server machines, the cables connecting them and all supporting hardware in between such as bridges, routers and switches. In wireless systems, antennas and towers are also part of the network.

Software: Instructions for the computer. A series of instructions that performs a particular task is called a "program." The two major categories of software are "system software" and "application software." System software is made up of control programs such as the operating system and database management system (DBMS). Application software is any program that processes data for the user (inventory, payroll, spreadsheet, word processor, etc.). See system software and application software. Software tells the hardware how to process the data.

World Wide Web (WWW): A major service on the Internet. The World Wide Web is made up of "Web servers" that store and disseminate "Web pages," which are "rich" documents that contain text, graphics, animations and videos to anyone with an Internet connection. The heart of the Web technology is the hyperlink, which connects each document to each other by its "URL" address, whether locally or in another country.

1.0 PREAMBLE

The SWLSB seeks to provide its staff, students, stakeholders and visitors with secure and timely access to IT equipment and the online services and resources necessary for undertaking their work and learning. Consequently, the School Board is highly reliant on information that is gathered, stored, processed and delivered by computers and their associated communications facilities. The purpose of this Policy is to give a clear statement to all users of the SWLSB IT facilities and services of their responsibilities, including what constitutes appropriate use; to manage the provision and modification of access to online services; and to express the commitment of the School Board to providing and maintaining a secure, effective and reliable IT infrastructure to support the School Board`s operations.

2.0 OBJECTIVES

2.1 Promote responsible use of information and communication technology resources;

2.2 Protect the integrity of information and communications systems and equipment;

2.3 Provide rules to all users who wish to use the Sir Wilfrid Laurier School Board information technology resources including equipment, access to corporate network, Internet, e-mail and IP telephony;

3.0 PRINCIPLES

3.1 Information and communication technology resources are provided to students and personnel in all SWLSB schools, centres and departments to support educational and administrative activities and facilitate communication and access to information;

3.2 The school board under the Loi sur l'accès aux renseignements personnels des organismes publics et sur la protection des renseignements personnels must safeguard the personal information of its employees and students. Personal information cannot be disclosed without the person's permission. For students under 18, parental consent is required;

3.3 The Sir Wilfrid Laurier School Board believes that pertinent user education and the provision of the relevant and useful information available on the internet are the best ways to support the effective use of technology.

3.4 The Sir Wilfrid Laurier School Board has measures in place to restrict access and filter inappropriate materials; however, those measures do not provide foolproof protection and users may access or receive inappropriate materials either intentionally or unintentionally. Requests to block or unblock content must be approved by the School Administrator or School Board Service Director. Due to security concerns the Director of Information Technology has the final authority before any content is blocked or unblocked. For a category list of appropriate content please see Annex D.

3.5 The Sir Wilfrid Laurier School Board reserves the right to monitor or investigate all ICT activities for inappropriate use or for performance statistics including e-mail correspondence, web navigation and phone activity that are carried out on its network by all stakeholders.

3.6 In the context of an investigation, the Board may be requested to present information stored or communicated by a user without prior notice.

3.7 The SWLSB reserves the right to block or filter any network traffic that potentially breaches this policy or is potentially illegal;

3.8 Only authorized users may access computer resources, and only within the usage limits allowed by the School Board. Use of this privilege must be reasonable and must not unduly reduce other users' access to computer resources.

3.9 The Sir Wilfrid Laurier Code of Conduct (Policy 2011-HR-08) applies at all times while using ICT resources from within the School Board's network or from locations outside the Sir Wilfrid Laurier School Boards' buildings.

3.10 The School Board will ensure that safety is a priority in regards to our wireless infrastructure. The School Board will continue to follow Health Canada (Health Canada Safety Code 6 - http://www.hc-sc.gc.ca/ewh-semt/pubs/radiation/radio_guide-lignes_direct/index-eng.php) and other local health authorities' guidelines and make any adjustments necessary to ensure the safety of our stakeholders.

4.0 SCOPE OF APPLICATION

4.1 USERS

This policy applies to all school board employees, students of the youth and adult sectors, commissioners, parents, volunteers, consultants, service providers and any authorized guest using the board's ICT resources. This policy also applies to ICT users who have access to the board's ICT resources from home and/or outside regular work/school hours.

4.2 RESOURCES

This policy applies to the following ICT resources: servers, workstations, peripherals, telecommunications equipment including telephone equipment, software, software packages, information and data banks, all internal or external computer communications networks owned or leased by the School Board, controlled or administered by the School Board, or over which the School Board holds right of usage.

4.3 ACTIVITIES

This policy applies to all pedagogical or administrative activities conducted with ICT Resources by ICT users.

- Consequences of misuse and abuse shall result in the suspension of privileges to access Information and Communication Technology Resources and may lead to disciplinary and/or legal action including liability costs.

5.0 RESPONSIBILITIES

The School Board will take all reasonable steps to protect its IT facilities and services from unauthorised and unacceptable use.

5.1 The Council of Commissioners is responsible for the adoption and revision of this policy.

5.2 The Director General is responsible for the application of this policy.

5.3 The Director of the Information Technology Department is responsible for the implementation of the policy.

5.4 Schools and centres administrators are responsible for the application of this policy in their school or centre. To that effect schools and centres administrators are to:

- Monitor the use of information technology resources;
- Secure parental consent for access to network resources through the Student User Agreement for students under 18;
- Inform all users of the policy on an annual basis.

5.5 All users must conform to this policy and abstain from inappropriate use of information and communication technology resources.

- Consequences of misuse and abuse shall result in the suspension of privileges to access Information and Communication Technology Resources and may lead to disciplinary and/or legal action including liability costs.

5.6 All users must sign a User Agreement (*Annex A, B or C*).

5.7 All SWLSB IT hardware, especially portable devices, must be kept secured at all times against damage, misuse, loss or theft. In addition, hardware and software containing sensitive information or data must be protected with appropriate security measures such as passwords or PIN codes.

5.8 SWLSB IT Storage hardware that becomes obsolete must be disposed of in a manner that renders any information illegible and irretrievable at the time of disposal.

6.0 RESPONSIBLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY RESOURCES

When using the Sir Wilfrid Laurier School Board's ICT resources users must at all times:

6.1 Report all inappropriate use, breach of security, and unsolicited content to their teachers or immediate supervisor;

6.2 All SWLSB account holders must adhere to the SWLSB password rules outlined in the Procedure for Password Security.

6.3 Remain within their specifying access rights to resources;

6.4 Use the equipment at their disposal safely, diligently and with proper care;

6.5 Use the ICT resources for educational, professional and administrative purposes;

6.6 Maintain the integrity of systems (e-mail, storage spaces, servers) by respecting the resources limits and by regularly deleting or archiving files and e-mails;

6.7 Protect personal and confidential information of the school board and other organizations;

6.8 All users have an individual and a shared responsibility in protecting academic and business data against unwanted disruptions, loss of sensitive data as outlined in the *Act respecting access to documents held by public bodies and the protection of personal Information* (*http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=%2F%2FA_2_1%2FA2_1_A.htm*), or unauthorized access and use. Therefore, all users must take responsibility for their own individual choices to use cloud applications in connection with their role at SWLSB. Specifically, it is the responsibility of the individual using cloud services to ensure that their use is in compliance with all School Board policies and procedures.

6.9 As part of the application of this policy, the Sir Wilfrid Laurier School Board may conclude contracts with external persons or companies. The Sir Wilfrid Laurier School Board cannot be held responsible for any consequences that would result from a breach or fault by the external person or company.

7.0 INAPPROPRIATE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY RESOURCES

When using the Sir Wilfrid Laurier School Board's ICT resources users must refrain at all times to:

7.1 Alter, damage or destroy ICT equipment;

7.2 Destroy or alter the integrity of personal data and the information of other users;

7.3 Post personal information about themselves or others without proper authorization. Personal information includes but is not limited to name, phone number, address, pictures and video clips;

7.4 Use ICT resources for personal financial gains or for posting goods and services;

7.5 Users of the SWLSB IT facilities and services must not create, send, store, upload, access, use, solicit, publish or link to;

7.5.1 Offensive, obscene, profane or indecent images or material (other than for properly authorized, supervised and lawful education or research purposes, in which case an appropriate warning must be given).

7.5.2 Material likely to cause harassment, or intimidation to some individuals or cultures.

7.5.3 Discriminating or sexually harassing material or messages that create an intimidating or hostile work or study environment for others.

7.5.4 Defamatory material or material that makes misrepresentations or could otherwise be construed as misleading.

7.5.5 Material that infringes the intellectual property (including copyright) of another person or organization.

7.5.6 Malicious software such as viruses, malware, ransomware, worms or address-harvesting software.

7.6 Intrude in other users' files without proper authorization;

7.7 Login under other users' names and passwords;

7.8 Deliberately attempt to disrupt the network performance and security, damage or alter data, spread viruses and other harmful means;

7.9 Modify, copy or transfer software without authorization and appropriate licensing;

7.10 Send global messages, chain letters, or any other type of communications, which can cause congestion on the network.

8.0 PROVISION FOR REVIEW

This policy shall be reviewed when deemed necessary.

COMMISSION SCOLAIRE SIR-WILFRID-LAURIER
SIR WILFRID LAURIER SCHOOL BOARD

Policy nº 2000-IT-01:	Procedure for Password Security

All SWLSB systems must have appropriate user IDs and passwords to ensure access is restricted only to authorized individuals.

The SWLSB requires that wherever possible, strong passwords must be used (see below for examples). Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Punctuation
  - “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
- Contain at least eight (8) alphanumeric characters

Weak passwords have the following characteristics:

- The password contains less than eight (8) characters
- The password is a word found in a dictionary
- The password is a common usage word such as:
  - Names of accounts, family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "swlsb", "wilfrid", "swlaurier", "swlauriersb" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

One way to create strong passwords is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

1.0 Password rules for SWLSB Staff:

- It must be a minimum length of 8 characters;
- It must contain at least two different character types (ex. Upper & lower case, Letters & symbols…);
- Must be changed every 90 days or when prompted to do so;

Must be changed immediately by the user or the Information Technology Department if there is a possibility that the password may have been compromised.

2.0 Password rules for SWLSB Students:

- It must be a minimum length of 6 characters;
- It must not be your network account name (ex. User: 0123356 Password: 0123456);
- Each student's password will be reset by the Information Technology Department prior to the start of the school year.

3.0 Password safety for all users;

It is recommended that all SWLSB users follow these best practice guidelines concerning passwords:

- Do not reveal your password to ANYONE. Do not reveal a password to co-workers while you may be on vacation. The IT Department will never request your password so please disregard any requests via email for your password;
- If someone demands your password, refer him or her to this document or the SWLSB Information Technology Department;
- Do not use the" Remember Password" feature of applications or web sites;
- Do not write passwords down and store them anywhere where they are easily found by others;
- Avoid reusing a password. The use of a password manager (ex. Dashlane, Keeper Password Manager) is recommended for those who have multiple unique passwords to remember.

ANNEX A

COMMISSION SCOLAIRE SIR-WILFRID-LAURIER
SIR WILFRID LAURIER SCHOOL BOARD

Elementary Student User Agreement and Parent Consent

- When using school computers, I will use appropriate language and not look at or use anyone else's work without permission;
- I shall not give out personal information such as my address, telephone number, parents' work addresses or telephone numbers, credit card;
- I shall not give out the name and address of my school without permission from a staff member or teacher;
- I shall tell my teacher right away if I come across any information that is inappropriate or makes me feel uncomfortable;
- I shall never send my picture or anything else without first checking with my parents and /or teacher;
- I shall not give out my password to anyone (even my best friends);
- I shall never agree to get together with someone I "meet" on-line;
- I shall talk with my parents about the rules for going on-line;
- I understand that anyone can read messages I send and that my work on the computer is not private;
- I have read and I understood the rules and promise to follow them. If I do not follow these rules I know that I may have my computer privileges restricted or taken away.

Student's School: _____

Grade: _____

Student Name (please print): _____

Student Signature: _____

Date: _____

Date of Birth: _____

A complete version of the Policy is available on the School Board Web site at www.swlauriersb.qc.ca

Parent / Guardian Consent

As the parent / guardian of the above named student, I have read and I have understood the Policy on the Use of Information and Communication Technology Resources. I grant permission for my son / daughter / charge to access networked services such as e-mail and the Internet.

Name of Parent / Guardian (Please Print): _____

Signature of Parent / Guardian: _____

Date: _____

ANNEX B

COMMISSION SCOLAIRE SIR-WILFRID-LAURIER
SIR WILFRID LAURIER SCHOOL BOARD

Under 18 (High School, Adult and Vocational Training) Student User Agreement

- When using school computers, I will use appropriate language and not look at or use anyone else's work without permission;
- I shall not give out personal information;
- I shall keep my password confidential and not give out to anyone;
- I understand that anyone can read messages I send and that my work on the computer is not private;
- I understand that my online activities (digital footprint) are permanent and not always private;
- I shall not download or share any copyrighted materials that I do not have the rights to;
- I have read and I understood the rules and agree to follow them. If I do not follow these rules I know that I may have my computer privileges restricted or taken away at any time.

Student Agreement

I have read and I have understood the Policy on the Use of Information and Communication Technology Resources. I agree to abide by it and understand that any violation of any provision may result in the loss of access privilege and school sanctions.

Student's School or Centre: _____
Level or Program: _____
Student's Name (please print): _____
Student's Signature: _____
Date: _____
Date of Birth: _____

Student's Signature: _____

A complete version of the Policy is available on the School Board Web site at www.swlauriersb.qc.ca

Parent / Guardian Consent

As the parent / guardian of the above named student, I have read and I have understood the Policy on the Use of Information and Communication Technology Resources. I grant permission for my son / daughter / charge to access networked services such as e-mail and the Internet.

Name of Parent / Guardian (Please Print): _____

Signature of Parent / Guardian: _____

Date: _____

ANNEX C

COMMISSION SCOLAIRE SIR-WILFRID-LAURIER
SIR WILFRID LAURIER SCHOOL BOARD

User Agreement

User Agreement

I have read and I have understood the Policy on the Use of Information and Communication Technology Resources. I agree to abide by it and understand that any violation of any provision may result in the loss of access privilege and/or sanctions.

Name (Please Print): _____

School, Centre or Department: _____

Signature: _____

Date: _____

ANNEX D

COMMISSION SCOLAIRE SIR-WILFRID-LAURIER
SIR WILFRID LAURIER SCHOOL BOARD

Internet Filtering List

The following is a list of Internet categories and how the SWLSB filters each.

Deny Access

Adult Materials
Child Abuse
Dating
Discrimination
Drug Abuse
Explicit Violence
Extremist Groups
Freeware and Software Downloads
Gambling
Games
Hacking
Illegal or Unethical
Lingerie and Swimsuit
Malicious Websites
Marijuana
Nudity and Risqué
Phishing
Pornography
Proxy Avoidance
Spam URL
Sports Hunting and War Games
Spyware and Malware
Tasteless
Tobacco
Weapons (Sales)

Allow Access

Abortion
Advertising
Advocacy Organizations
Alcohol
Alternative Beliefs
Armed Forces
Arts and Culture
Child Education
Brokerage and Trading
Business
Content Servers
Digital Postcards
Domain Parking
Dynamic Content
Education
Educational Games
Entertainment
File Sharing and Storage
Finance and Banking
Folklore
General Organizations
Global Religion
Government and Legal Organizations
Health and Wellness
Information and Computer Security
Information Technology
Instant Messaging
Internet Radio and TV
Internet Telephony
Job Search
Medicine
News and Media
Newsgroups and Message Boards
Personal Vehicles
Personal Websites and Blogs
Plagiarism
Political Organizations
Real Estate
Reference
Restaurant and Dining
Search Engines and Portals
Secure Websites
Sex Education
Shopping and Auction
Social Networking
Society and Lifestyles
Sports
Streaming Media and Download
Travel
Web-based Applications
Web-based Email
Web Chat
Web Translation
Web Hosting