Appropriate Use of Information Technologies
GSA.F.3

Adopted: August 22, 2011
Last Reviewed/Revised: November 14, 2011

Purpose

This policy outlines the appropriate use of information technology for board employees, students and service providers.

References

- *Municipal Freedom of Information and Protection of Privacy Act*
- *Ontario Health Information Protection Act*
- Ontario Student Record Guidelines
- *Ontario Personal Health Information Protection Act*
- *Ontario Libel and Slander Act*

Forms

- Form 1: Employee/Service Provider to the Board
- Form 2: Student Use of Technology

Appendices

- Appendix A: Examples of Unlawful Activity

Policy Statement

The Wellington Catholic District School Board (the "Board") provides authorized employees, students, and service providers with access to the Board's electronic information and technology systems, electronic mail, internet, and voice mail systems.

With prior permission employees, students, and service providers may also be allowed to use non-Board technology (personal devices such as cell phones, smart phones, laptops, tablets etc.) on Board premises.

The Board is committed to ensuring that the use of technology on Board premises is for proper work-related purposes, or to support learning, in a manner that is not detrimental or harmful to the interests of others. Use of technology on Board premises must not compromise the confidentiality or proprietary nature of information belonging to the Board. The board reserves the right to monitor all usage, regardless of the ownership of devices and to take disciplinary measures as required, if inappropriate use is detected. Information accessed using technology on Board premises must be consistent with the Mission Statement of the Board and the Gospel values we believe.

Policy Regulation

1. General

1.1. The Board maintains electronic mail, internet, and voice mail systems as part of its technology platform. The Board may also authorize employees, students, or service providers to utilize non-Board owned technology. The use of any technology on Board premises must be to assist in the conduct of Board business and should only be utilized as directed or outlined by the Board.

1.2. When using Board provided technology including Board e-mail or internet services, all email and internet communications sent and received by users are the property of the Board. E-mail, internet, or voice-mail communications are not private or personal despite any

such designation by the sender or the recipient. Personal or private communications transmitted on the Board's electronic information system may be accessed, reviewed, copied, deleted, retained, or disclosed by the Board at any time and without notice.

1.3. The Board reserves the right, without prior notice to the employee, student, or service provider, to monitor the use of technology on Board premises. Board owned technology provided to an employee, student, or service provider, may be accessed or recalled without any prior notice.

1.4. The right of the Board to access an employee, student, or service provider's e-mail, internet, or voice-mail on Board provided technology or servers, or to disclose the contents may arise in a number of situations, including:

- to comply with disclosure requests or orders made pursuant to the *Municipal Freedom of Information and Protection of Privacy Act*;
- for Board owned technology, because of regular or special maintenance of the electronic information systems;
- for Board owned technology, when the Board has a business-related need to access the employee's system, including, for example, when the employee is absent from work or otherwise unavailable;
- in order to comply with obligations to disclose relevant information in the course of a legal proceeding; and when the Board has reason to believe that there has been a violation of this policy, or the use is incompatible with the Board's mission as a Catholic School Board.

1.5. For Board owned technology; the Board recognizes that some personal use is inevitable, provided that it is not in violation of this policy. Regardless of ownership, it is against this policy to use the Board's technology for excessive personal use. Excessive personal use includes but is not limited to installing and using bit torrents, downloading movies and games, etc. and any other such personal use that consumes high bandwidth. Users acknowledge that

personal use information is not privileged or protected by privacy legislation and users explicitly waive any privacy rights they may have or claim under the *Municipal Protection of Privacy Act* or any other relevant legislation, federal or provincial.

1.6. Information posted to the internet from a Board facility must comply with the *Municipal Freedom of Information and Protection of Privacy Act*, Board guidelines, and be consistent with the policies and Mission of the Board.

1.7. Establishing or accessing websites, links, postings, email messages, text messages, or any form of publishing which has an unauthorized connection to the School Board or which may be criminal, degrading, defamatory or inappropriate is expressly forbidden and in violation of this policy. The author will be required to remove such material as soon as it is identified as being in violation of this policy and further action may be taken against the author.

1.8. From time to time, employees or service providers will have access, or have in their possession electronic versions of student data. It is the employee's and service provider's responsibility to safeguard that data under the Ontario Student Record Guidelines and if applicable, the *Municipal Freedom of Information and Protection of Privacy Act* and/or the *Ontario Health Information Protection Act*. Employees or service providers who suspect that this data has been compromised shall notify their immediate supervisor or the board's Superintendent of Corporate Services.

1.9. Except with the prior approval of the appropriate supervisory officer, employees, students and service providers may not establish internet or external connections that could allow unauthorized access to the Board's computer systems and information. These connections include (but are not limited to) the establishment of multi-computer file systems, ftp servers, telnet, internet relay chat or remote control software.

2. Prohibited Activities

The following clauses apply to all Board owned technology regardless of location, and to any technology while on Board premises regardless of ownership:

2.1. It may not be used to store, distribute, post, download, or view any defamatory, abusive, obscene, profane, pornographic, sexually oriented, threatening, racially or ethnically offensive, sexist or illegal material.

2.2. It may not be used to transmit or distribute the Board's confidential or proprietary information in a manner that would constitute negligence.

2.3. It may not be used for any unlawful activity, examples of which are outlined in Appendix A.

2.4. Transmission and use of any unlicensed software, software having the purpose of damaging computer systems or files (e.g. computer viruses), software that compromises the integrity of the systems (e.g. key loggers, password sniffers) is prohibited. All software and files downloaded must be systematically checked for viruses before loading on Board technology systems.

2.5. Any malicious attempt to harm, destroy, or illegally access data of any person, computer, or network linked to the Boards Wide Area Network (WAN) is prohibited.

2.6. The use of camera phones is strictly forbidden in private areas: locker rooms, washrooms, dressing areas, at any time. Such use may be in violation of the Criminal Code and Privacy legislation and may be subject to internal and external disciplinary consequences.

3. Guidelines and Application

3.1. Human Resource Services will ensure all new staff acknowledges they have read and understood the policy (and related documentation) and will place a signed copy of the acknowledgement form in the employee's personnel file. Compliance with the policy is a condition of employment.

3.2. All students shall read and sign this policy (and related documentation) prior to accessing the Internet, using any board technology, or bringing any devices on Board premises. If a student is under 18 years of age, a parent or guardian shall also sign the policy. This may be done as part of the student's registration process.

3.3. An electronic acknowledgement of the policy may also serve as the official record in lieu of a paper copy.

3.4. Principals will notify parents about the existence of this Appropriate Use of Technology Policy, and will require that students and their parent/guardian sign this policy prior to the student accessing the Internet, using any board owned technology or bringing any personal devices on Board premises.

3.5. Principals will establish the steps to be taken by students and staff to respond to any violation of the policy, including if applicable the inadvertent access in the school to inappropriate/illegal material on the Internet.

3.6. Principals and the relevant ICT personnel must be informed of any serious infraction of this policy. Disciplinary actions will be handled in accordance with the discipline policies of the Board and the school.

3.7. Teachers shall provide students with instruction on the appropriate use of the Internet and the protocols for the use of electronic mail. If other electronic communications or technology methods are to be used they shall be accompanied by instruction on appropriate use

and associated risks. Teachers shall ensure that students accessing the Internet do so as part of an instructional plan.

3.8. Parents and or Guardians agree that they have read and understood the board's Appropriate Use of Technology policy and have explained the same to their children or ward and that they will emphasize the ethical and responsible use of technology and caution against inappropriate use.

3.9. By signing this policy (and related documentation), Parents and or Guardians grant permission for their child or ward to access networked information technology, inclusive of the internet and e-mail. If a Parent or Guardian does not wish for their child or ward to access networked information they shall inform the Principal in writing.

3.10. Parents and or Guardians agree to fully cooperate with the Board and any relevant investigating authority, should a serious infraction of the policy occur due to the use of non-Board owned technology, on Board premises.

3.11. Failure to comply with this Policy may result in the loss of access privileges, financial compensation to the Board, pursuance of criminal charges, and/or other disciplinary action up to and including discharge.

3.12. Network Etiquette

All users of e-mail, voice mail, and the internet should abide by generally accepted rules of etiquette, including the following:

- Be polite. Do not be abusive in your exchanges with others.
- Use appropriate language. The use of abusive, harassing, or profane language is prohibited.
- Do not post chain letters or engage in "spamming".

3.13. Security and Personal Safety

All users of e-mail, voice mail, and the internet should abide by generally accepted rules of security and personal safety, including the following:

- Users may not share their passwords or accounts with others and must make all efforts to safeguard this information from unauthorized users.
- Users are advised to refrain from giving out personal information, such as their family name, email address, home address, school name, city, country or other information that could help someone locate or contact them in person.
- Users will not post identifying photos or videos.

4. Terms and Definitions

Spamming

Spamming refers to sending an annoying or unnecessary message to a large number of users.

Wellington Catholic DISTRICT SCHOOL BOARD FAITH IN EDUCATION

Appendix A

Examples of Unlawful Activity

For the purpose of this policy, "inappropriate use" and "unlawful activity" is interpreted broadly and includes any criminal activity or other illegal activity.

The following are examples of "inappropriate use" "unlawful activity" for the purpose of the policy:

Pornography	• possessing, downloading or distributing any pornography.
Intellectual Property	• infringing on another person's copyright, trade mark, trade secret of any other property without lawful excuse.
Other Criminal Activity	• using technology as a means to commit criminal activity (examples include but are not limited to fraud, extortion, sale and/or purchase of restricted goods).
Defamatory Libel	• A matter published without lawful justification or excuse, that is likely to injure the reputation of any person by exposing that person to hatred, contempt or ridicule, or that is designed to insult the person. - *The Libel and Slander Act, RSO 1990, Chapter L.12.*
Disclosing or Gathering Personal Information	Personal Information

	• Disclosing personal information in a manner inconsistent with the *Municipal Freedom of Information and Protection of Privacy Act.*
Hacking and Other Crimes Relates to Computer Systems	Examples include (but are not limited to): • Gaining unauthorized access to a computer system. • Trying to defeat the security features of network connected devices. • Use of software and/or hardware designed to intercept, capture and/or decrypt passwords. • Intentionally spreading a computer virus. • Destroying or encrypting data without authorization and with the intent of making it inaccessible to others with a lawful need to access it. • Interfering with other's lawful use of data and technology.
Harassment	• Using technology, without lawful authority, to cause people to fear for their safety or the safety of anyone known to them.
Hate Propaganda	• Communicating messages that promote or incite hatred against an identifiable group that is likely to lead to a breach of the peace.
Inception of Private Communications or Electronic Mail (In Transit)	• Unlawfully intercepting someone's private communications or unlawfully

	intercepting someone's electronic mail.
Obscenity	• Distributing, publishing or possessing for the purpose of distributing or publicly displaying any obscene material

Form 1

Employee/Service Provider to the Board

New Employee/Service Provider to the Board

As a user / service provider of the Wellington Catholic District School Board's technology services, I have read the Wellington Catholic District School Board's Policy *Appropriate Use of Technology* and its related documentation, *GSA. F.3.,* and agree to abide by it.

_____

Name (Printed)

_____ _____

Signature Date

_____ _____

Witness Date

Information Collection Authorization:

A current version of the policy and regulations, *GSA. F.3.,* is available on the board web site at www.wellingtoncdsb.ca under the policies section.

The personal information contained on this form has been collected under the authority of the *Education Act R.S.O. 1980, C.129*, as amended and the *Municipal Freedom of Information and Protection of Privacy Act, 1989.*

This form will be handled with the strictest confidence. Questions about the collection of this information should be directed to the school principal or to the Wellington Catholic District School Board's Freedom of Information/Protection of Privacy at (519) 821-4600.

COPIES: (1) HR File / ICT File (2) Employee / Service Provider (upon request)

Wellington Catholic DISTRICT SCHOOL BOARD FAITH IN EDUCATION

Form 2

Student Use of Technology

Student Consent – Primary – Junior – Intermediate (Grades JK – 8)

I agree to:

- Use all technology equipment carefully and not damage, change or tamper with the hardware, software, settings or the network;
- Keep my password secret;
- Use the technology only to help me learn;
- Give credit to the author of work I find on the internet and obey copyright laws;
- Not provide my personal information (name, address, phone number) to anyone on the internet;
- Never meet in person with someone I have met online without my parent's approval and participation;
- Tell my teacher or any other school employee about anything on the computer or other devices that is inappropriate or makes me feel uncomfortable;
- Never use any form of technology to harass, frighten, or bully anyone;
- Take care when printing and consider the environment when deciding what to print.

_____
Student Name (Printed)

_____ _____
Student Signature Date

Student Consent – Intermediate – Senior (Grades 9 – 12)

I agree to:

- I have read and understood Wellington Catholic District School Board's (the Board's) *Appropriate Use of Technology* and its related documentation, *GSA. F.3.*, and recognize that it is governing my use of the technology on Board premises and that these documents are available on the board's website
- To abide by the policy and recognize that failure to comply with the policy may result in the loss of computer and/or network access privileges, financial compensation to the Board and other disciplinary actions consistent with the *School's Code of Behaviour*, Board Policy and/or legal authorities.

_____

Student Name (Printed)

_____ _____

Student Signature Date

Parent/Guardian Consent

- I have read and understood the Wellington Catholic District School Board's *Appropriate Use of Technology* and its related documentation, *GSA. F.3.*;
- I recognize that the full policy and related documentation governing my child's use of technology is available on the board's website or from my child's school;
- I will emphasize the ethical and responsible use of technology and caution my child about unsafe communication with others on the internet;
- I grant permission for my child to access networked information technology, inclusive of the internet and e-mail for educational purposes. I am aware that my child will be given instruction in the proper use of the internet at school and further recognize

that I am responsible to supervise my child's use of the computer and internet at home;

- I agree to fully cooperate with the Board and any relevant investigating authority, should a serious infraction of the policy occur due to the use of non-Board owned technology, on Board premises.

_____

Parent/Guardian Name (Printed)

_____ _____

Parent/Guardian Signature Date

Information Collection Authorization:

A current version of the policy and regulations, *GSA. F.3.*, is available on the board web site at www.wellingtoncdsb.ca under the policies section.

The personal information contained on this form has been collected under the authority of the *Education Act R.S.O. 1980, C. 129*, as amended and the *Municipal Freedom of Information and Protection of Privacy Act, 1989*.

Information from this form will be used to enforce appropriate use of technology. Questions about the collection of this information should be directed to the school principal or to the Wellington Catholic District School Board's Freedom of Information/Protection of Privacy at (519) 821-4600.

COPIES: (1) Student File (2) Parent (upon request)