

YORK CATHOLIC DISTRICT SCHOOL BOARD



BOARD POLICY	
<i>Policy Section</i> Program/Curriculum	<i>Policy Number</i> 311
<i>Former Policy #</i> 220	<i>Page</i> 1 of 5
<i>Original Approved Date</i> January 15th, 2002	<i>Subsequent Approval Dates</i> October 11th, 2011

POLICY TITLE: STUDENT ACCEPTABLE USE OF INFORMATION TECHNOLOGY

SECTION A

1. PURPOSE

The York Catholic District School Board (the “Board”) is committed to safe, equitable and productive use of Information Technology to enhance learning for all students within a Christ-centered school environment.

2. POLICY STATEMENT

It is the policy of the York Catholic District School Board to provide and maintain Internet and Information Technology access in support of student learning that is consistent with the Board Vision Statement, Catholic values, and Ministry guidelines.

3. PARAMETERS

- 3.1 The Board recognizes the importance of maintaining the confidentiality of all users of its Information Technology facilities and assets without compromising the ability to regulate, enforce and promote acceptable use guidelines.
- 3.2 Students using the Board information technology, whether at school or remotely, must adhere to strict ethical and lawful conduct in compliance with Board rules and policies.
- 3.3 All students and parents/guardians will sign annually the grade appropriate Student Acceptable Use of Information Technology Agreement (Forms S36, S36a, S36b) prior to accessing Board information technology, either at school or remotely.
- 3.4 Students downloading, uploading or sharing information using the Board information technology, whether in school or remotely, will observe and respect any material that is protected by copyright, patent, trademark, service mark and other applicable laws.
- 3.5 Students accessing Board Information Technology resources are prohibited from engaging in inappropriate or unlawful activities whose examples are listed in, but not limited to Appendix A.
- 3.6 Allegations of unlawful or unacceptable use of the Board information technology will be addressed through established Board policies and procedures and, where necessary, disciplinary actions taken in accordance with Safe Schools (Student Discipline, Policy # 202).
- 3.7 All on-line internet correspondence and interactions between students and staff must be directly related to ongoing coursework or school sanctioned activities.

4. RESPONSIBILITIES

4.1 Director of Education

- To ensure the implementation of this policy throughout the Board.

4.2 Supervisory Officers

- To work with school administrators to ensure that all sections of this policy are implemented and adhered to.

4.3 Instructional Services

- To provide resources that will support the appropriate and ethical use of information technology by students.

4.4 School Principal or designate

- To notify the school staff, the students and the parents/guardians of the Student Acceptable Use of Information Technology Policy.
- To require all students and parents/guardians to sign the appropriate Student Acceptable Use of Information Technology Agreement as specified: JK-3 (Form S36), 4-8 (Form S36a), 9-12 (Form S36b).
- To retain records of the Student Acceptable Use of Information Technology Agreements.
- To ensure that school staff is aware of their responsibilities for supervising and monitoring student access to the internet to enhance learning and teaching.
- To inform all staff that online internet correspondence and interaction between staff and students must be directly related to ongoing coursework or school sanctioned extra-curricula activities
- To review and approve school-based online social media activities and groups that are linked to instructional plans and supervised by school staff.
- To ensure that school-based online social media groups have at least one staff member with administrative privileges to review, screen and modify contents to conform to the Student Acceptable Use of Information Technology Policy.
- To inform the staff supervising online social media activities and groups to adhere to ethical standards for the teaching profession in the same manner as in traditional school environment.
- To establish the steps to be taken by students and staff when inappropriate and/or illegal internet contents are accidentally accessed by a student to ensure the safety of the child.
- To cooperate fully with ongoing investigation by Board staff, the police and other authorities into illegal activities or crime that may have been committed while using the Information Technology systems and network of the Board.

4.5 School Staff and Classroom Teachers

- To link the use of the internet and related applications such as interactive websites and social media groups to ongoing coursework, unit plans and curriculum related learning. Prior to permitting students to use the internet as part of an ongoing lesson, the teacher should ensure that there is clear written instruction outlining the goal for such a use and that the students understand the parameters.
- To review and evaluate the suitability of internet learning resources and websites prior to permitting students to have access online.
- To monitor online internet use within interactions and social media activities of all students under supervision.

- To provide students with instruction at the beginning of each school year on the safe and appropriate use of Information Technology and the internet.
- To communicate clearly to students the consequences of inappropriate/illegal use of Information Technology that may include discipline by the school, the Board and Police services.
- To report to the school principal any breach of internet policy, and inappropriate use of Information Technology

4.6 Students

- To report to staff in the school when images, material or information on the Internet make them uncomfortable.
- To report to staff in the school when pornographic sites are accidentally accessed.
- To report to staff in the school when a stranger attempts to initiate contact, interaction or conversation on the Internet.
- To respect the Student Acceptable Use of Technology Policy at all times when in school and/or when using school computers and internet.
- To report to staff in the school when they become aware that another student is illegally/inappropriately using Board technology resources.
- To be respectful technology users who care about equipment and about other students who use the same technology.

5. DEFINITIONS

5.1 Information Technology

- all forms of technology, portable and non-portable, used to create, store, transmit, and use information in all its forms including but not limited to data, audio, images, motion pictures, multimedia presentations, and other forms (including future inventions and applications) within and outside YCDSB.

5.2 Intellectual property

- property developed or created in the course of employment or by contractual agreement, and in the absence of a written agreement to the contrary, is owned by the YCDSB.

5.3 Internet

- the global communication system that enables information to be transmitted, received, stored and exchanged through the World Wide Web (www) by a user or group of users using applications such as e-mail and social media.

5.4 Intranet

- the internal network of communication servers owned, operated and regulated by the YCDSB.

5.5 Social media

- interactive online applications such as Facebook, Twitter, Youtube, blogs, wikis et cetera where people are talking, participating, sharing, networking, and may be accessed by the wider internet community (Please see YCDSB Web-based Technology and Instruction Guidelines).

5.6 Student Acceptable Use of Information Technology Agreement (Forms S36, 36a 36b)

- standard form signed by students and their parents/guardians agreeing to abide by the YCDSB's Student Acceptable Use of Information Technology Policy.

5.7 Unlawful activity

- any illegal use of YCDSB information technology. Examples are listed in but not limited to Appendix A.

Unacceptable/Unlawful Use of YCDSB Information Technology

The following is a partial list of examples that includes but is not limited to activities considered unacceptable/unlawful.

Bullying	An attempt to undermine an individual through cruel and humiliating behaviour, including 'cyber-bullying' which is using the internet/intranet to send threatening, obscene, sexually explicit and violent messages that threaten emotional and physical safety of recipient(s).
Child pornography	Accessing, downloading, storing, sharing and distributing any child pornography
Copyright or trademark infringement	Infringing on another person's copyright, trademark, patent, trade secret, without lawful permission
Defamatory libel	A defamatory libel is matter published, without lawful justification or excuse, that is likely to injure the reputation of any person by exposing him/her to hatred, contempt or ridicule, or that is designed to insult the person of or concerning whom it is published. <i>Libel and Slander Act</i> .
Disclosing or gathering personal information	Disclosing or gathering personal information in a manner inconsistent with the <i>Municipal Freedom of Information and Protection of Privacy Act</i> .
Gambling and lotteries	Uploading funds to online gambling or lottery sites, making bets or playing the games that they offer, and then cashing out any winnings
Hacking and other unauthorised access	Includes but not limited to using the computer to carry out sabotage, gain unlawful entry into encrypted sites, acquiring and disseminating private information, creating and disseminating computer viruses, stealing information and trade secrets, engaging in delinquent game of breaching protected internet sites that compromises the safety of others.
Harassment	The sending of electronic messages and information that cause the recipient(s) to fear for personal safety and that of others.
Hate propaganda	Communicating messages that promote or incite hatred against an identifiable group that is likely to lead to a breach of the peace—e.g. homophobic messages, racist comments and jokes, violent gender-specific messages.
Inappropriate communication with minors	Communicating, soliciting or sending sexually suggestive, emotionally laden, and intrusive personal messages to minors for any reason.
Intellectual property	Infringing on another person's property without lawful permission.
Interception of private communication or electronic mail	Unauthorised entry into the password protected e-mail and/or the interception of private electronic communication intended for someone else
Obscenity	Creating, acquiring, sharing, publishing and distributing any obscene material including pornography.
On-line Video Gaming	Participating in on-line "video gaming", while using YCDSB information technology equipment.
Personal financial gains	Any use of Board information technology for commercial transactions, advertising, solicitation and financial gain.
Vandalism	Deliberately damaging or causing to be damaged Board information technology, for example routers, modems, wireless et cetera including but not limited to physical technology equipment, internet /intranet resources, online traffic flow, internet filters and firewalls, websites etc...