YORK CATHOLIC DISTRICT SCHOOL BOARD

BOARD POLICY	
Policy Section **Program/Curriculum**	*Policy Number* **311**
Former Policy # **220**	*Page* **1 of 8**
Original Approved Date	*Subsequent Approval Dates*
January 15th, 2002	**October 11th, 2011** **November 26, 2013** **October 29, 2019**

POLICY TITLE: DIGITAL DISCIPLESHIP
STUDENT USE OF TECHNOLOGY

SECTION A

1. PURPOSE

The York Catholic District School Board (the "Board") is committed to safe, secure, equitable and effective use of technology to enhance learning for all students within a Christ-centered school environment. In support of its ongoing commitment to excellence in Catholic Education and to ensure that all become responsible digital disciples of the 21st century, the Board regulates the use of technology on all school board premises, and during sanctioned activities.

2. POLICY STATEMENT

It is the policy of the York Catholic District School Board to regulate the use of technology including personal devices while fostering a healthy learning environment using good digital discipleship in a safe, respectful and positive manner, guided by gospel values that are consistent with the Board's Mission, Vision, Core Values and Ontario Catholic School Graduate Expectations.

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 The York Catholic District School Board reserves the right to monitor, access and disclose all data and information created, sent and received, processed or stored on Board information technology systems to ensure compliance with Board policies.

3.3 Students using technology and personal devices:

3.3.1 Shall abide by the York Catholic District School Board Policy 218 Code of Conduct and respect the need of others to work in an environment that is conducive to learning and teaching;

3.3.2 Are prohibited from engaging in inappropriate or unlawful activities whose examples are listed in, but not limited to Appendix A. Allegations of unlawful or unacceptable use of technology will be addressed through established York Catholic District School Board policies and procedures and, where necessary, disciplinary actions taken in accordance with Safe Schools (Policy 202 Safe Schools - Student Discipline).

3.4 The responsibility to keep all board technology and personally owned electronic devices secure and maintained shall rest with the owner. York Catholic District School Board is not liable for any personal device lost, stolen or damaged.

3.5 Use of personally owned electronic devices on Board/School Premises and during Board/School sanctioned events shall be as outlined:

3.5.1 For health and medical purposes;,

3.5.2 To support special education needs;,

3.5.3 For educational purposes, as directed by an educator.

3.6 Students using technology, whether downloading, uploading or sharing information at school or remotely, shall observe and respect any material that is protected by copyright, patent, trademark, service mark and other applicable laws and adhere to strict ethical and lawful conduct in compliance with the Board's Mission, Vision, and Core Values.

3.7 Access to the York Catholic District School Board wireless network is a privilege, not a right. Any use of the wireless network shall entail personal responsibility and compliance with all York Catholic District School Board policies and school expectations or guidelines.

3.8 Access to the York Catholic District School Board wireless network shall be content filtered to safeguard against inappropriate content.

3.9 Users of personally owned devices shall make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.

3.10 With respect to personal devices, including personal medical devices (PMDs), the Board cannot guarantee the availability of Internet services or security of devices. PMD users should not rely upon the security and availability of the District's internet connections and wireless network services. PMD users with continuous, critical needs should arrange for their own redundant, secure communication systems.

3.11 Students and Parent(s)/Guardian(s) shall sign the technology consent form prior to accessing Board technology, either at school or remotely on an annual basis.

3.12 Students accessing technology and resources understand that the Board retains ownership of intellectual property, where the Board's resources or expertise are used to create a product or practice that may have commercial significance.

3.13 All electronic communications and social media interactions between students and staff must be directly related to coursework or school sanctioned activities.

4. RESPONSIBILITIES

4.1 Director of Education

4.1.1 To oversee compliance with the Digital Discipleship, Student Use of Technology Policy.

4.2 Superintendent of Curriculum & Assessment

4.2.1 To support the implementation and compliance with the Digital Discipleship, Student Use of Technology policy.

4.2.2 To review annually the Digital Discipleship, Student Use of Technology policy, with school administrators.

4.3 Chief Information Officer

4.3.1 To oversee, in collaboration with the Superintendent of Curriculum & Assessment the implementation and compliance with the Digital Discipleship, Student Use of Technology policy.

4.3.2 To oversee, in collaboration with relevant services such as legal, privacy and risk management, appropriate procedures and guidelines are established to assist board employees to fulfill their responsibilities as set out in this policy.

4.4 Manager of Employee Relations & Privacy

4.4.1 To oversee, in collaboration with the Chief Information Officer, appropriate implementation of and compliance with the Digital Discipleship, Student Use of Technology policy.

4.5 Senior Administration

4.5.1 To work with school administrators to ensure that all sections of the Digital Discipleship, Student Use of Technology policy are implemented.

4.6 Instructional Services

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

4.7 Principal

4.7.1 To communicate with school staff, students and Parent(s)/Guardian(s) the Digital Discipleship, Student Use of Technology policy.

4.7.2 To require all students and Parent(s)/Guardian(s) to sign the annual Technology Consent Forms.

4.7.3 To retain records of the Technology Consent Forms.

4.7.4 To inform all staff that electronic communication and interaction between staff and students must be directly related to school based activities.

4.7.5 To ensure that school staff are aware of their responsibilities for supervising and monitoring student use of technology and electronic communications.

4.7.6 To review and approve school-based online social media activities and groups that are linked to instructional plans and supervised by school staff.

4.7.7 To ensure that school-based online social media groups have at least one staff member with administrative privileges to review screen, monitor and

modify contents to conform to the Digital Discipleship, Student Use of Technology policy.

4.7.8 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 a traditional school environment.

4.7.9 To offer support to students who accidentally accessed unacceptable internet content. Administrators will offer school/area/board support, based on the developmental needs of the student.

4.7.10 To report any security, safety or privacy related breach or issue relating in any unacceptable activities and violations that may have been committed.

4.7.11 To cooperate fully with ongoing investigation by Board staff, the police and other authorities into unacceptable activities and violations that may have been committed while using the technology systems of the Board.

4.8 Staff

4.8.1 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.

4.8.2 To review and evaluate the suitability of internet learning resources and websites prior to permitting students to have access online.

4.8.3 To monitor school related online internet use within interactions and social media activities of all students under supervision.

4.8.4 To provide students with instruction at the beginning of each school year on the safe and acceptable use of technology and the internet.

4.8.5 To communicate clearly to students the consequences of inappropriate unacceptable use of technology that may include discipline by the school, the Board and Police services.

4.8.6 To be responsible technology users who take necessary online safety and security precautions when sharing information with others online or on Cloud Drives such as Google Drive.

4.8.7 To report to the school principal when they become aware of any security, safety or privacy related breach or issue.

4.8.8 To report to the school principal any breach of the policy, and inappropriate use of technology.

4.9 Students

4.9.1 To adhere to the Digital Discipleship, Student Use of Technology policy at all times when in school and/or when using school computers and internet.

4.9.2 To report to staff in the school when they become aware that another student is hacking or illegally/inappropriately using technology resources.

4.9.3 To report to staff in the school when they become aware of a security, safety or privacy related breach or issue.

4.9.4 To be responsible digital disciples who take necessary safety and security precautions when sharing information with others online or on Cloud Drives such as Google Drive.

4.9.5 To be respectful digital disciples who care about equipment and about other students who use the same technology.

4.9.6 To report to staff in the school when images, material or information on the internet make them uncomfortable.
4.9.7 To report to staff in the school when pornographic sites are accidentally accessed.
4.9.8 To report to staff in the school when a stranger attempts to initiate contact, interaction or conversation on the internet.

4.10 Parent(s)/Guardian(s)

4.10.1 To review with their child the Annual Technology Consent Forms and to sign and submit them to the school in a timely manner.
4.10.2 To cooperate with the school to ensure that their child complies with this policy and the use of personal electronic devices only as direct by teachers/Principal.
4.10.3 To understand that any violation may result in the loss of privileges as well as disciplinary action.
4.10.4 To discuss with the Principal any extenuating circumstances where their child is required to have access to a personal electronic device, such as a cellphone, outside of educational purposes, including the use of personal medical devices (PMD).

4.11 Volunteers, Third Party Providers and Visitors

To be aware and comply with the Digital Discipleship, Student Use of Technology policy.

5. DEFINITIONS

5.1 Cloud Drive

Digital technology, any of several, often proprietary, parts of the Internet that allow online processing and storage of documents and data as well as electronic access to software and other resources.

5.2 Digital Discipleship

Guided by our Catholic values, one who uses technology ethically and responsibly to advocate for local and global issues, act in solidarity and stewardship and promote human dignity

5.3 Hacking

The unauthorized practice of accessing, modifying or altering computer software, hardware, or networks to accomplish a goal that is considered to be a security breach and outside of the creator's original objective.

5.4 Illegal activity

Any illegal use of the York Catholic District School Board technology. Examples are listed in, but not limited to, Appendix A.

5.5 Technology

Includes, but is not limited to, personal electronic devices, personal medical devices (PMD), board network and infrastructure, electronic communication equipment such as laptops, desktops, mobile devices, robotics, printers and audio/video equipment.

5.6 Intranet

The internal network of communication servers owned, operated and regulated by the York Catholic District School Board.

5.7 Personal Electronic Device

Includes any device in the possession of a student which electronically communicates, sends, receives, stores, reproduces, or displays voice, text, and/or digital communications or data. This includes, but is not limited to, cellular phones, pagers, smart phones, music and media players,
gaming devices, tablets, laptop computers, cameras, video cameras, smart watches, headphones, earbuds, personal medical devices (PMDs), and personal digital assistants. In this policy, the word "technology," may be used as a synonym for personal electronic device,

5.8 Sanctioned Activities

The legitimate and authorized use of a personally owned electronic device during activities which may include, but are not limited to, specific programming purposes, lengthy bus excursions, co-curricular events, inclement weather and/or, legitimate medical reasons. Such use must be authorized by Administration and/or staff.

5.9 Social Media

Any interactive online where people are talking, participating, sharing, networking, and may be accessed by the wider internet community.

6. CROSS REFERENCES

YCDSB Policy 112 Privacy and Personal Information Management
YCDSB Policy 113 Intellectual Property
YCDSB Policy 116 Copyright
YCDSB Policy 202 Safe Schools - Student Discipline
YCDSB Policy 218 Code of Conduct
YCDSB Policy 223 Bullying Prevention & Intervention
YCDSB Policy 317 Electronic Communications & Social Media

YCDSB Digital Discipleship Framework
YCDSB Visual Identity and Branding Manual

Child and Family Services Act
Copyright Act
Criminal Code
Education Act
Human Rights Act
Municipal Freedom of Information and Protection of Privacy Act

7. RELATED FORMS

YCDSB Annual Technology Consent Form

Approval by Board	**October 29, 2019**
	Date
Effective Date	**October 30, 2019**
	Date
Revision Date	**October 29, 2019**
	Date
Review Date	**October 2024**
	Date

Appendix A

Unacceptable/Illegal Use of York Catholic District School Board Electronic Communications & Social Media

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

Bullying	An attempt to intimidate an individual through cruel and humiliating behaviour, including 'cyber-bullying' which is used 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. *Libel and Slander Act.*
Disclosing or gathering personal Information	Disclosing or gathering personal information in a manner inconsistent with the *Municipal Freedom of Information and Protection of Privacy Act.*
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 unauthorized access	Includes but not limited to using the computer to carry out sabotage, gain illegal entry into encrypted sites, acquiring and disseminating private information, creating and disseminating computer viruses, stealing information and trade secrets, intentionally breaching protected internet sites that compromises the safety of others.
Harassment	The sending of electronic messages and information that causes 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 email and/or the interception of private electronic communication intended for someone else
System Security/Account Security	Users are responsible for the use of their individual account and should take reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person.
Obscenity	Creating, acquiring, sharing, publishing and distributing any obscene material including but not limited to pornography.
On-line Video Gaming/Gambling	Participating in on-line "video gaming," which is not associated to classroom learning is prohibited; and/or all on-line gambling, while using information technology.
Personal financial gains	Any use of Board information technology for commercial transactions, advertising, solicitation and financial gain.
Threat	Communication through the use of mail, email, telephone, telegram, or other instrument of commerce; the willful making of any threat; or the malicious conveyance of false information knowing the same to be false which concerns an attempt being made, or to be made; to kill, injure, intimidate any individual; or unlawfully to damage or destroy any building, vehicle, or other real or personal property by means of an explosive.
Vandalism	Deliberately damaging or causing to be damaged Board information technology, for example routers, modems, wireless, etc., including but not limited to physical technology equipment, internet /intranet resources, online traffic flow, internet filters and firewalls, distributed denial of service (DDOS), websites etc…
Technology/Equipment	York Catholic District School Board Information Technology and/or Personal Electronic Devices used for anything outside of educational purposes is prohibited.