CATHOLIC DIOCESE OF YOUNGSTOWN

Office of Catholic Schools

CI-30 Student Technology and Internet Acceptable Use Policy

The schools in the Diocese of Youngstown, acquire, develop, and maintain devices, information and communication resources, systems, and networks as a part of our mission to promote excellence in education. The following policy aims to ensure that safety and privacy are regarded and students' educational experiences are enhanced through the use of technology. It is the belief of the Diocese that students' productivity, efficiency, effectiveness, creativity, and the preparation for future studies and endeavors is achieved through innovative practices while using technology.

Protecting users and school resources requires respectful, moral, and ethical behavior characteristic of the teachings and principles of the Roman Catholic Church. This policy specifies the expectations that allow for a safe, and courteous environment, where academic integrity is honored, and respectful behavior is demonstrated in regard to communication with members, and the use of school devices, resources, and the components of the network, both locally and globally. The policy also addresses legal responsibilities of members** and institutions.

Although no set of policies and procedures can state rules to cover all possible situations, the schools in the Diocese make efforts to protect the users and its system through educating students about Internet safety and by using firewalls and filtering software. We are in compliance with the *Child Internet Protection Act and The Protecting Children in the 21st Century Act.* However, no system or network is considered full-proof.

Important Considerations

- Technology resources are to be used for educational purposes only.
- Local school's policies, related Diocesan policies, and the Student Code of Conduct concurrently apply.
- Users are subject to legal requirements as well. (See link to Ohio Revised Code §§ 2917.21(A), 2913.01(Y)
- The policy applies to access to the Internet through the school network whether equipment is owned by the school *or the student or student's family.*
- The policy applies to access to the Internet with personally owned devices with personal data plans (i.e. 4G and 5G networks).
- Students are responsible for all activity performed using *a personal login* or account, *whether or not they were the user*. Therefore, students must take care to *safeguard passwords* and follow procedures. If students become aware of, or suspect any breach of an account, they must notify a teacher, administrator, or technology coordinator of the suspected breach.
- In some instances, the policy applies to technology resources whether or not on school property. (See the section: Violations of the Acceptable Use Policy)
- Students are to refrain from posting material on social media that may adversely impact school operations, and/ or disrupt the school environment.
- Students and a parent or guardian, as stated, are required to sign the Acceptable Use Policy Agreement in order to agree with compliance of the code of practice.

- The use of school systems and equipment is a privilege and use may be revoked by an administrator, technology coordinator, or other designated school official for misuse or violation of the policy.

Related to Safety

By signing this policy, *a student of the Diocese of Youngstown agrees to not:*

- interfere with, adversely impact the school operations, detract from or disrupt the school environment, as determined by school administration, by using technologies in a way that could jeopardize the safety or well-being of a school member or group bully, tease, embarrass, offend, proposition, threaten, harass, deceive, or intimidate (cyberbully) school members* whether directly or as a forwarded message. This includes using school members' names, initials, logos, pictures, or representations when communicating electronically that, in the determination of the school administration, are degrading, lewd, threatening or inappropriate, including but not limited, to comments, cartoons, jokes, unwelcome propositions or love letters.
- bypass or attempt to bypass school security software or attempt to use an alternate server including personal data plans.
- send personal information about self or a school member* via a school account.
- attempt to open files or follow links from an unknown or untrusted origin.
- view violent, obscene or similar inappropriate material. If inappropriate content is accidentally accessed, the student must notify the supervising school staff immediately to avoid potential consequences.

Related to Privacy

By signing this policy, *a student of the Diocese of Youngstown agrees to not:*

- use a student or staff, password to access an account.
- access or attempt to access files or accounts, including G-Suite applications, belonging to another student or school employee without express permission from the owner.
- take pictures or record video, and/or audio on school property without the express permission of a school staff member and persons involved. Parental permission may also be required.
- use and/or publish a photograph, image, video, personal information or likeness of any student, or diocesan employee without the express permission of that individual. Parental permission may also be required. Last names should always be omitted. See reference to the *Children's Online Privacy Protection Act.*
- hide one's identity and/or pretend to be a school member* and communicate via email, or messaging apps, photos, or videos.
- create any website, blog, or wiki and post identifying information, a photo, image, video, or work of a school member* except with the express permission of that individual and a school official. Parental permission may also be required. The use of last names should always be omitted when posting on the Internet. Students should be careful to not share personally-identifying information online. (See link to the *Children's Online Privacy Protection Act* and to *Ohio Revised Code* §§ 2917.21(A), 2913.01(Y))

Related to Educational Integrity

By signing this policy, *a student of the Diocese of Youngstown agrees to not:*

- use diocesan and school created email and G-Suite applications for communications unrelated to schoolwork.
- access social networking sites or gaming sites or apps, except for educational purposes, and with the permission and supervision of the responsible school official.
- access websites or apps while taking online quizzes or tests without a teacher's prior approval.**

- use a device while taking a quiz or test without a teacher's prior approval.**
- transmit or share information or images of quizzes or tests through texting, photography, or any other electronic means without a teacher's prior approval.**
- access or attempt to access private school record-keeping software, including, but not limited to, online grade books, attendance software, report card/transcript records.**
- delete files, deny or attempt to deny school member* from gaining access to their files or work.
- use the intellectual property of others including fellow students or teachers, to share, copy, plagiarize, and/or profit, without proper citation and express permission from the owner.
- use any copyrighted material, including text, music, software, files, pictures, or graphics from any Internet or software source in violation of United States Fair Use copyright laws.
- violate program or software license agreements (i.e. modify, copy, share protected media).

Related to Network and Systems Stability and Privacy

By signing this policy, *a student of the Diocese of Youngstown agrees to* ***not:***

- attempt to open files or follow links from an unknown or untrusted origin.
- remove, install, load, or execute programs and/or files not expressly authorized by the school official responsible.
- remove, move, alter or add equipment without express authorization from the school official responsible.
- access or attempt to access unauthorized devices, accounts, websites, or information databases (e.g. hacking, cracking, phishing, etc.).
- damage, destroy, or remove any piece of hardware, program, or network equipment without proper authorization. This includes willfully disseminating computer viruses.
- attempt to interfere with network transmissions or change system configurations.

Students, keep in mind that nothing in an email or posted on the Internet is considered private. High school students should be aware that employers, college admissions directors and recruiters look at students' Internet posts when considering applicants.

Teaching staff and administration has the right to deny a student access to applications provided by the school that are used for collaborative projects and social networking if conduct is offensive, interferes with student learning, or affects fellow students' well-being.

School and diocesan administrators reserve the right to monitor, inspect, copy, review, save and store any information on devices and the computer systems and network including Internet data shared on the school systems and network, at any time and without notice, whether using personally owned or school owned technologies.

*Student, school or diocesan staff

** Consequences for academic cheating may also apply.

<u>Violations of this Acceptable Use Policy</u>

School officials will strive for a fair, reasonable, and appropriate disciplinary action for infractions of the Student Technology and Internet Acceptable Use Policy. Disciplinary action will be taken when, violations are intentional, school members* are 'cyberbullied', vandalism has occurred, or any action involves criminal behavior. Consequences may include but are not limited to: detention, termination of Internet or technology privileges, revocation of financial aid and scholarships, suspension, expulsion, or legal referral. Behavior that occurs on or off school property can be considered for investigation and consequence when it interferes with, adversely impacts school operations, or disrupts the school environment.

Social Media

In the event students use social media applications such as, but not limited to, Instagram@, Snapchat@, Twitter®, Youtube@, or FaceBook®, for public scandal or humiliation, where inappropriate defamatory, threatening, or socially and/or emotionally harmful comments or images are posted that adversely affect the reputation, the morale, and/or safety of the students, staff, and institution, every disciplinary measure deemed appropriate, will be used. Actions could include legal action, involvement of law enforcement officials, suspension, or recommendation for expulsion of the student(s) involved.

Liability

The Diocese of Youngstown and its schools have taken available precautions to use firewalls and filters to restrict/limit access to controversial materials. Students and their parents are alerted to the risks of the Internet and the use of technologies. However, on a global network it is impossible to control all communication and materials.

It cannot be guaranteed that functions and services provided by the schools operate error free or without defect. Therefore, The Diocese of Youngstown and its schools will not be held liable for loss of data and interruptions of service. The Diocese of Youngstown and its schools will not be responsible for damage or harm to any personal devices, files, data or hardware brought to school by students. The Diocese of Youngstown and its schools will not be responsible, financially or otherwise, for costs arising from unauthorized use of the systems or network, for unauthorized transactions conducted over the school network, or for any communications or transactions in violation of this Student Technology and Internet Acceptable Use Policy.

Links and Supporting Resources

A. Children's Internet and Protection Act and Protecting Children in the 21st Century Act
http://transition.fcc.gov/cgb/consumerfacts/cipa.pdf
See part (4) (A) and (B) Children's Online Privacy Protection Act (COPPA)
http://www.coppa.org/coppa.htm
Copyright Law and United States Fair Use
http://www.copyright.gov/fls/fl102.html
"What should I know about my children's Internet use?"
https://www.ohiobar.org/ForPublic/Resources/LawFactsPamphlets/Pages/LawFactsPamphlet-23.aspx
Internet and Social Media: A Legal Guide for Catholic Educators. Shaughnessy and Huggins.
Ohio Revised Code ORC § 3314.21 on web filtering
Ohio Revised Code §§ 2917.21(A), 2913.01(Y) on cyberbullying

B. School Code of Regulations

C. Related Diocesan Policies
Copyright
Educational Technology
Internet Safety
Personally Owned Device
Student Anti-Bullying, Harassment, and Intimidation
Student Code of Conduct

Revised: 6.1.2017