Office of Catholic Schools

CI-30 Student Technology and Internet Responsible Use Policy

The schools in the Diocese of Youngstown, provide information and communication resources, and acquire, develop, and maintain devices, systems, and networks as a part of our mission to promote excellence in education. The following agreement 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. Students in the Diocese of Youngstown will have access to the Internet. Parents are expected to encourage their child(ren) to exercise personal safety and security, and utilize the guiding principles of digital citizenship

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.
- Students will be educated in digital citizenship annually.
- 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 and school owned devices. whether or not on school property (See the section: Violations of the Responsible Use Agreement).
- The Student Technology and Internet Responsible Use Policy is contained in the Family Handbook. Students and a parent or guardian, as stated, are required to sign the Family Handbook Agreement Form which indicates acceptance of and compliance with this policy.
- 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 agreement.

Related to Safety

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 to intimidate (cyberbully), tease, embarrass, offend, threaten, harass, deceive, or impersonate school members* whether directly or indirectly. 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 or device security software or attempt to use an alternate server including personal data plans.
- send or post 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 while in school or while using school owned devices. If inappropriate content is accidentally accessed, the student must notify the supervising school staff immediately to avoid potential consequences.

Related to Privacy and Security

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 or within a remote learning environment 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 link to the Children's Online Privacy Protection Act (COPPA).
- 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 or blog 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))
- create accounts or use apps or sites for school business when under the allowable age as in terms for the app or website.

Related to Educational Integrity

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 while in a school session, 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 an unauthorized 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.**
- share passcodes and passwords for learning platforms unless given express permission by a teacher or administrator.
- 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 members* 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, video 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

A *student of the Diocese of Youngstown agrees to* ***not****:*

- attempt to open files or follow links from an unknown, suspicious, 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 must 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.

Violations of the Student Technology and Internet Responsible Use Policy

School officials will strive for a fair, reasonable, and appropriate disciplinary action for infractions of the Student Technology and Internet Responsible 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, TikTok, 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 in the school's Code of Conduct 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. Best efforts to avoid the collection and release of any student data for anything other than educational purposes will always carried out when using apps or websites. 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. Refer to the Children's Internet and Protection Act and Protecting Children in the 21st Century Act.

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 Responsible Use Policy.

Student Applications and Permissions

The use of technology in education is integrally related to a quality instructional program. The following items describe what platforms may be used. If a parent wants to opt out of any of the following, a written letter must be sent to the school principal indicating what the opt out request is and the reason for the request.

- **Google Apps for Education Account**
  All email passes through Google's Postini security system and students' school accounts are restricted to receiving correspondence **only from school or district account holders** unless it is requested by an administrator that select educational institutions or programs are granted access. Please read the privacy policies associated with use of Google Apps for Education at http://www.google.com/a/help/intl/en/edu/privacy.html. The account will also include access to cloud storage, document and information exchange with Google Drive, Google Classroom, Google Slides, Google Forms, Google Sheets, Google Calendar and Google Keep.)

- **Student Personally Owned Device Agreement**
  When students use a personally owned device at school, they must follow the terms of this policy when accessing the Internet. In addition, the student is responsible for safeguarding and maintaining the device.

- **Remote Learning Platform**
  While remote learning is seldom an optimal substitution for face-to-face instruction and interaction, continuing to instruct and communicate with your student is essential when circumstances occur where face-to-face instruction must be suspended. This could be due to a health crisis (ex. COVID 19) or another cause. Internet-based tools such as Google Meet and Zoom may be used for audio and video instruction. Platforms such as Class Dojo, See Saw, and Google Classroom may be used to share and receive information and assignments. Other approved educational web-based services, applications*** and websites may be used at the discretion of the teacher.

  In remote learning periods, a classroom teacher may conduct virtual classroom instruction. Video and audio may be used for teaching purposes, and at times may record classroom activities for educational use/ purposes. In the process of recording, a child's face may be seen, a voice may be heard. And a first name of a student may be used. The recordings will only be shared within the school setting for students unable to attend the virtual classroom activity in real time. The recordings will be stored, accessed, and disposed of within the confines of school accounts. Students are permitted to access such recordings within the school account in which they were distributed. They may not share or post to any other technology device or application.

  The school filters and restricts access to controversial materials from school computers. However, web-based content accessed outside the school could put the student in contact with objectionable materials. It is the responsibility of the parent/guardian to restrict any access to materials deemed inappropriate.

  Many of the Terms of Service and or Privacy Policies for ***some applications (e.g., Class Dojo, Remind,

Zoom) state that due to federal law, any users under the age of 13 must obtain parental permission. An email address and a first and last name may be required to create a username, however, students are not required to have their own account.

If remote learning is mandated due to a health crisis or other reason, the school will assist parents in providing access to a device or internet access. Participation in remote learning should be under the supervision of a parent or guardian. School policies and regulations are in effect, including, but not limited to this policy and the School Code of Conduct.

- **Photo/Visual Recording***

  A student may be photographed or videotaped at school. This includes the possibility of publishing a photo or video in a publication, on the school website, on social media platforms or another publication that is deemed appropriate for informational and instructional purposes. In addition, a child may be photographed for the class picture, the yearbook, and other school paper publications.

  At times students may be photographed for a community newspaper or for publications to be used outside of the school (ex. Marketing brochure).

  *Parents may send a letter to the school principal to opt out of any aspect of the Photo/Visual Recording.

- **Publishing of Student Material**

  Student work will be published within the confines of Google Classroom or another remote learning platform used by the school.

  A student's work material may be shared in publications, on the school's website, or other social media platforms under their first name and last initial.*

  If a full name of a student is required for publication of student work in a public communication, parent permission will be sought.

  *Parents may send a written request to the principal for a child to opt out of communications shared with the public.

Links and Supporting Resources

Children's Internet and Protection Act and Protecting Children in the 21st Century Act
https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

See part (4 A&B) Children's Online Privacy Protection Act (COPPA)
https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Copyright Law and United States Fair Use https://www.copyright.gov/fls/fl102.html"What should I know about my children's Internet use?"

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

Family Educational Rights and Privacy Act (FERPA) - https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

B. School Code of Regulations

C. Related Diocesan Policies

- Copyright
- Educational Technology
- Internet Safety
- Student Anti-Bullying, Harassment, and Intimidation
- Student Code of Conduct

Initial adoption: 5.30.13
Revised: 6.1.2017
7.28.2020