APPENDIX A

RESPONSIBLE USE POLICY FOR TECHNOLOGY

Catholic Schools of the Archdiocese of Philadelphia

Revised August 2024

Preamble

The heart of our curriculum is timeless— love, truth, beauty, and mercy. We teach about creation as well as the Creator. We educate on being in solidarity with those who suffer and how to cultivate a prayerful life. In his 48th World Communications Day message, Pope Francis said technology is a "gift from God." The Pope challenged the Church to use this tool to promote the faith, asking how communication can "be at the service of an authentic culture of encounter?" Because of these things, we are committed to participating in society. And to be committed to such participation requires using technology in appropriate ways.

We are interested in technology because of our faith. We expect our students to utilize technology to think more critically, to communicate effectively, to express their creativity, and to conduct research. Our teachers have access to updated technology in their classrooms to engage our students and challenge them to learn in ways not previously imaginable. We empower students with the technical skills necessary to participate in a culture increasingly dependent upon technology while challenging them to be digital ambassadors spreading the Good News. But it is our faith that guides how we use technology. We teach our students about the ethics of technology and train them to be savvy about things like Internet privacy and safety. We teach the unfortunate reality of technology addiction. We remind students and parents that technology is aggressively marketed and to be careful about getting caught up in the hype. We also acknowledge that we sometimes need to "unplug" from technology as it can cause us to become isolated from one another. We encourage family meals without screen time and the importance of communicating face-to-face. We greatly value technology in our schools. And what makes technology most powerful, is when it serves to make our students better people!

PURPOSE

Technology is a valuable educational tool. All Archdiocese of Philadelphia schools will educate all students about appropriate online behavior, including interacting with other

individuals on social networking websites and chat rooms, cyberbullying awareness, and response to ensure appropriate use of technology, including video conferencing platforms. The policy outlined below applies to all technology use, including but not limited to Internet use. The Responsible Use Policy for Technology (RUP) applies to all students, faculty, administrators, staff, volunteers, or community members allowed access to school technology resources.

SCOPE OF USE

We recognize that the digital world allows anytime, anywhere access. Uses mentioned in this policy apply to inside school use and may in certain instances apply to personal technology use and/or uses outside of school. Where personal and/or non-educational use of technology creates substantial disruption in school, including but not limited to harming or interfering with the rights of other students or teachers to participate fully in school or extracurricular activities, these activities may be viewed as a violation of the Responsible Use Policy and may be subject to the disciplinary measure found herein. NB. The types of electronic and digital communications referenced in this RUP include, but are not limited to, social networking sites, cell phones, mobile computers and devices, digital cameras, video conferencing platforms, text messaging, email, voice over IP, chat rooms, instant messaging, cloud, and web-based tools.

GOALS

The school's goal is to prepare its members for a responsible life in a digital global community. To this end, the school will:

- Integrate technology with curriculum to enhance teaching and learning.
- Encourage critical thinking, communication, collaboration, creativity, and problem-solving skills.
- Facilitate evaluation and synthesis of information.
- Encourage ethical practices and provide education for Internet safety, digital citizenship, and the creation of a positive digital identity.
- Provide a variety of technology-based tools and related technology skills.

USER RESPONSIBILITIES

Our schools will make every effort to provide a safe environment for learning with technology, including Internet filtering and safeguards. The students, faculty, administrators, staff, and school community are granted the privilege of using computer hardware and software peripherals and electronic communication tools, including the Internet. With this privilege comes the responsibility for appropriate use. In the

Archdiocese of Philadelphia (AoP), we use information and technology in safe, legal, and responsible ways. We embrace the following conditions or facets of being a digital citizen.

- Respect One's Self: Responsible users will select online names that are appropriate and will consider the information and images that are posted online.

- Respect Others: Responsible users will refrain from using technologies to bully, harass, or defame other people, school personnel, and other school-related images or likenesses.

- Protect One's Self and Others: Responsible users will protect themselves and others by reporting abuse and not forwarding inappropriate materials or communications. Users will protect their usernames and passwords by not sharing them with others.

- Respect Intellectual Property: Responsible users will suitably cite any and all use of websites, books, images, media, or other sources relied upon or used in work created.

- Protect Intellectual Property: Responsible users will request permission to use the software and media others produce and abide by license agreements for all software and resources.

- Under no circumstances is an AoP user authorized to engage in any illegal activity under local, state, federal, or international law.

TECHNOLOGY USE GUIDELINES

Educational Purpose/ Responsible Use: Technology is to be used to enhance student learning. Students are able to access social networking and gaming sites only under the guidance and supervision of the teacher for the educational outcomes identified within the lesson and given the appropriate age.

Copyright/Intellectual Property and Identity: All sources obtained for teacher and student work should be properly cited. Users are to respect the rights and intellectual property of others in accordance with Federal Copyright Law. Transferring copyrighted material to or from a school without express permission of the owner is a violation of
Federal law could result in copyright infringement claims.

Responsible Use of School-Utilized Hardware/Devices: All AoP users are responsible for the general care of school-utilized hardware, devices, and peripherals. Users shall report any damage to the school's hardware or device to the local school tech or school administrators as soon as possible. Local school policy may further define faculty, staff, and students' responsibilities and expectations. Users may be held liable for any costs associated with device repair or replacement.
Communications: Electronic and/or Digital communications with students should be conducted for educationally appropriate purposes and employ only school-sanctioned means of communication. The school-sanctioned communications methods include:

- School-created teacher web pages, school-issued email and/or school phone number
- Teacher created, educationally focused websites
- Student Information System and Learning Management System
- Remind Communication app—or similar i.e. Class Dojo, Seesaw

In their normal responsibilities and duties, teachers, administrators, or staff members may be required to contact parents outside of the school day. A teacher, administrator, or staff member may choose to contact parents or guardians using their home phone or a personal cell phone. However, they should not distribute or publish a home phone number or a personal cell phone number. If a student contacts a teacher or administrator using a teacher or administrator's personal numbers, email, or social networking sites, the teacher or administrator shall immediately report this to the administrator or appropriate authorities.

*** Teachers, staff, faculty, and school administrators may not use a personal email address for any school communications or school-associated account creation. The use of a personal email address is a direct violation of this policy, and the consequences may include loss of legal protection, a formal written warning, and/or possible dismissal/ termination. ***

Digital Security: Digital security must be at the forefront of every user's mindset. All users should always enable the highest level of account security offered. Typically, this means enabling two-factor authentication or multi-factor authentication to increase security. Biometric security features such as fingerprints or face IDs may also be utilized to protect an account from unauthorized access. It is strongly recommended that users use two-factor authentication on both school and personal internet accounts.

All staff, administrators, and teachers at the 15 Archdiocesan high schools and 3 schools of special education must enable and utilize two-factor authentication to log into their school-issued accounts.

Storage Devices: The use of external removable hard drives, flash drives, or "thumb" drives is strongly discouraged due to the possibility of information loss, theft, and other digital security concerns. The limited use of external drives in special circumstances may be allowed as long as specific attention is given to the security of these devices.

Artificial Intelligence: Students are prohibited from utilizing AI software tools such as ChatGPT for any academic or assessment-related purposes, including but not limited to completing assignments, quizzes, or exams. A student may use AI tools only if a teacher or school administrator explicitly gives permission and supervises its use. The unauthorized use of ChatGPT or other similar AI programs to complete school assignments is a violation of academic integrity and is subject to disciplinary action. Responsible users will not use ChatGPT or another program to create materials and submit them as their own original
work. Note— Many of these AI programs require users to be at least 13 years of age for use. Schools should thoroughly research the AI programs' Privacy Policy to check for compliance with COPPA, FERPA, and CUPA laws before introducing AI programs for student use. The AoP Tech Team is happy to help evaluate any AI tools or programs.

Electronic and Mobile Devices, Cell Phone, Wearable Technology: Users must adhere to local school policy that may further define uses of mobile devices. The administrator of the local school will determine permissible use. If a particular mobile device is to be used for an educational purpose, the school administration and/or teacher will provide parameters for this use.

Smart Speakers: Primarily intended for at-home consumer use, these always-listening devices are not directly intended for the classroom. Therefore, smart speakers (Echo, Google Nest, etc..) are not to be used in the classroom nor connected to the network on a permanent basis during the academic year.

Remote/Asynchronous/Distance Learning: Remote or distance learning may be used to supplement face-to-face instruction or, where appropriate, may be the primary modality of instruction. To effectively engage in remote or distance learning, users are expected to:

- Participate from an appropriate location in the home.
- To the user's best ability, be in a well-lit and quiet area. Avoid having windows or strong sources of light directly behind an individual when engaging in teaching/learning on camera.
- Wear appropriate and respectful attire. (This may be more specifically defined by the local school administration.)

- Where able, only use first name and last initial to identify yourself via video conferencing software.
- Students are not to use or preserve a photograph, image, video, including live streaming, or likeness of any student or employee without express permission of that individual and of the principal.
- Prior to recording any portion of a live classroom session, instructors are to notify the students who are in the same session, face-to-face or online.
- Live class recordings are meant for internal school use only. Recordings are to be saved locally on a network drive or the school's GSuite for Education Google Drive. Recordings are to be deleted at the end of the academic year in which they were recorded. Recordings are not for promotional use, rather solely for educational purposes.
- This Responsible Use Policy applies to students using either school-issued or personal devices.
- Maintaining hardware/devices provided by the local school is the responsibility of the student/family. (Local school policy may define further students' responsibilities and expectations.)

SPAM/PHISHING EMAIL REPORTING POLICY FOR AOP HIGH SCHOOLS

- All users should forward any suspect phishing or malware emails to: techsupport@[yourschooldomain]
- Do NOT click on any embedded links contained within a suspect email.
- Do NOT download or open any attachments included with any suspect email.
- Please alert the local school tech if any links were inadvertently clicked on or if any attached files were downloaded or opened.

AUDIO/VIDEO RECORDING

The below outlines the prohibition of unauthorized audio or video recording on school grounds and during school-related activities. This policy protects the privacy of students, staff, and families while fostering a safe and trusting learning environment.

Prohibited Activities:

- Recording of any classroom lesson, meeting, or school event without the prior consent of all participants, including from any involved students, teachers, or faculty members is forbidden.
- Prior to any audio or video recording, consent must be obtained from the classroom teacher, appropriate school administrator, and/or, when applicable, from the student's parents and guardians.

- Recording phone calls with school personnel, including teachers, administrators, or counselors, without prior notification and consent is forbidden.
- Using any recording device, including smartphones, tablets, iPads, Chromebooks, or other dedicated recorders, to capture unauthorized audio in classrooms, common areas, or during school functions is forbidden.

Exceptions

Educational Recordings: Teachers may utilize audio or video recording for approved instructional purposes, such as student presentations or language learning activities, after obtaining the required permission as mentioned above.

Consequences of Violation

Violations of this policy by students may result in disciplinary action, following the student code of conduct. Violations by staff will be addressed through appropriate administrative channels.

EXAMPLES OF UNACCEPTABLE TECHNOLOGY USES

RUP violations can include, but are not limited to, the following examples:

- Use technology to harass, threaten, deceive, intimidate, offend, embarrass, annoy, or otherwise negatively impact any individual.
- Post, publish, disseminate, or display any defamatory, inaccurate, violent, abusive, profane, or sexually-oriented material.
- Users must not use obscene, profane, lewd, vulgar, rude, or threatening language.
- Users must not knowingly or recklessly post or disseminate personal and/or false information about any person, student, staff, teacher, administrator, or any other member of the school community or school-connected organization.
- Use a photograph, image, video, including live streaming, or likeness of any student, administrator, employee, volunteer, school image, or logo without the express permission of that individual and the principal.
- Create any site or post any photo, image, or video of another individual except with the express permission from both that specific individual as well as from the school administrator.
- Attempt to circumvent system security, blocked sites, or software protections. This includes using personal or cell phone-based hotspots.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an

intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, 'disruption' includes, but is not limited to, network sniffing,

- pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the user, unless this activity is a part of the users normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Any virus or phishing protection software installed on school-utilized devices must not be disabled or bypassed.
- The use of any other login credentials other than those assigned to that specific user.
- Deliberately visit a site known for unacceptable material or any material that is not in support of educational objectives.
- Students must not access social networking sites or gaming sites except for educational purposes under teacher supervision.
- Violate license agreements, copy disks/hard drives, CD-ROMs, or other protected media.
- Use technology for any illegal activity. Use of the Internet for commercial gains or profits is not allowed from an educational site.
- Breach confidentiality obligations of school community members.
- At all times, users shall take all reasonable precautions to refrain from
- transmitting, sharing, posting, or otherwise divulging any confidential information, including, but not limited to, Individual Education Plans, 504 plans, donor or alumni information, financial documentation, test scores, demographic information, personnel files or information, grades, addresses, and other personal contact information.
- Harm the goodwill and reputation of the school or school system. This includes, but is not limited to, the misuse of school images and logos, the creation of unauthorized accounts that suggest they are school-sanctioned, or accounts targeting or impersonating school community members.
- Transmit any material in violation of any local, federal, and state laws. This includes, but is not limited to, copyrighted material, licensed material, and threatening or obscene material.
- Attempt to modify software and/or hardware configurations on a school-utilized device without proper permission and direction.
- Any attempt to alter data, the configuration of a school-utilized device, or the files of another user without the consent of the individual, building
- administrator or technology administrator will be considered a violation and subject to disciplinary action in accordance with the local school policies.

- Load personal software onto a school device or school-issued device without proper permission or direction.
- Attempt to make repairs to school-issued devices without proper permission and direction.

Reporting: Users must immediately report any damage or change to the school's hardware/software that is noticed by the user.

Administrative Rights: The school has the right to monitor the usage of school computers and digitally accessed content for all teachers, staff, administrators, students, and volunteers. Due to the evolving nature of technology, the Archdiocese of Philadelphia's Office of Catholic Education reserves the right to amend or supplement this policy at any time without notice.

All users are reminded that all computers, network traffic, and internet usage will be monitored. There is no assurance of privacy nor warranty of any kind, expressed or implied.

Usage of Social Media

This section of the policy refers to social media sites such as, but not limited to: Facebook, X (formerly Twitter), YouTube, Instagram, Steam, Ask.fm, Snapchat, Discord, Twitch, LinkedIn, and TikTok.

Teachers and students may not mention members of the school community on social media without their consent unless the subject is of public concern and the speech falls under applicable constitutional protections. This includes: Posting or sharing a teacher's, school personnel's, or another student's confidential information on public sites or any other unauthorized sharing with the intention to harm/harass.

Examples:

- Posting teachers' personal information, such as their personal email addresses, personal phone numbers, or addresses.
- Sharing a fellow student's phone number without their knowledge and consent to harass, threaten, deceive, intimidate, offend, embarrass, annoy, or otherwise negatively impact any individual.
- Manipulating or editing a teacher or student's photo in an inappropriate manner.

"Friending" or "Following" of current students by teachers is forbidden on a teacher's personal social media site. Teachers should also not 'friend' former students unless and until such student has attained the age of majority. Personal and professional posts must use appropriately respectful speech and refrain from harassing, defamatory, abusive,
discriminatory, threatening, or other inappropriate communications.

Teachers are encouraged to have professional social media accounts, separate from any personal account. Parents are encouraged to follow those for announcements and resources. Teachers are to inform local administrators as to any class utilizing social media, which should be for educational purposes only. In order to ensure the privacy and security of all students, teachers should refrain from posting on social media any audio, photo or video recording that captures a student's face or voice without prior parental authorization.

Permission must be obtained in advance from school administration for recording on school grounds, outside of the school day and/or school-sponsored events with the intent to post on personal social media accounts or non-sanctioned school accounts. Social media postings from school-sanctioned accounts should refer to students by their first name and last initial. Schools should NOT link or tag posts to students' personal accounts.
School-sponsored organizations must obtain permission from the school administration to create any social media accounts related to the organization. Such accounts should be created with a school-issued email account. Accounts should be maintained and controlled by a minimum of two school-appointed adult moderators.

In regards to student athletes and coaches:

- No coach, teacher, or administrator is permitted to have access to or control of a student's personal social media account.
- Students should never include their email or cellphone number in their social media bios.
- A student's personal social media account should not be tagged or linked to when posting social media messages.
- Coaches may want to post specific highlights, game/season achievements, or accolades on either the coach's professional page or a school's social media page. Students should be mentioned by first name only.
- Per the PIAA bylaws, students, teachers, and coaches shall not use social media to criticize contest officials or to promote rumors of questionable practices by opponents. Failure to follow this policy may result in disciplinary action.

Esports/Gaming Clubs

Esports or "electronic sports" refers to the world of organized, competitive video gaming. Unlike traditional sports, esports are virtual events that can be held both in-person and remotely. Though relatively young compared to other popular sports, the esports industry
may be a viable career option for avid gamers and is gaining participation at the collegiate level as schools seek to recruit student-athletes and join new competitions. Many colleges offer scholarships specifically for students interested in playing esports at the collegiate level.

School-sanctioned programs and gaming sessions should have, at minimum, one adult coordinator supervising the session, both if the team is meeting in person and when the team is meeting virtually.

Games rated E for Everyone or E 10+ are recommended for the Elementary grade level. At the Secondary level, games with a rating of E, E10, and Teen may be considered. Caution should be used when selecting games with a Teen rating as they may contain content that is only suitable for students ages 13 and over. Games rated as Teen may contain violence, suggestive themes, crude humor, minimal blood, and the infrequent use of strong language. Parents/Guardians should receive advance notice of game titles that will be used in the esports club. Parent/Guardian notice should include the game title, ESRB rating, and a link to Common Sense Media review or the ESRB rating review. Games rated higher than Teen are not recommended for Elementary school students.

For students playing esports at the Secondary level, games with a Mature (17+) rating must be cautiously evaluated by school administration. Students' parents and guardians should be notified prior to the game being played. Collegiate level esports programs often compete and may offer scholarships for games that are rated Mature (17+). These games often contain content that is only suitable for ages 17 and over, and content may contain intense violence, blood and gore, sexual content, and strong language. Extreme caution must be exercised if selecting a game that is either unrated or rated Mature. Some examples of popular esports games include:

(The following are examples only; their appearance here should not be considered approval or endorsement.)

Game Title	ESRB Rating	School Level
Call of Duty (COD)	Mature (17+)	Secondary
Counter-Strike: Global Offensive (CS: GO.)	Mature (17+)	Secondary

Defense of the Ancients (DOTA) and DOTA 2	Teen	Secondary
Fortnite	Teen	Secondary
Hearthstone	Teen	Secondary
League of Legends (LoL)	Teen	Secondary
Just Dance (2023, 2024)	Everyone	Elementary/Secondary
Mario Kart	Everyone	Elementary/Secondary
Minecraft	Everyone (10+)	Elementary/Secondary
Overwatch	Teen	Secondary
Player Unknown's Battlegrounds (PUBG)	Teen	Secondary
Pokemon (Sword & Shield)	Everyone	Elementary/Secondary
Rainbow Six Siege	Mature (17+)	Secondary
Rocket League	Everyone	Elementary/Secondary
Super Smash Brothers	Everyone (10+)	Elementary/Secondary
Sports Titles including MLB The Show, Madden, FIFA/EA Sports FC, NBA 2K	Everyone	Elementary/Secondary

For ratings of all games, please visit the ESRB website at esrb.org.

All school-sponsored esports activities must have the appropriate signed parental consent forms. The following permission forms are offered as templates that schools may use and may be customized for their specific needs.

Link to Sample Permission Form (Elementary)
Link to Sample Permission Form (Secondary)
Link to Sample Permission Form for specific games (K-12)

Parent permission must be granted for titles outside of the recommended ratings and for any game with a Mature rating. Permission for specific game titles is in addition to obtaining parent permission for overall esport club participation. Schools may decide to allow students to bring in their personal gaming systems or components for use in school in connection with an approved esports program. Schools must consider the security of the devices when they are not in use, the ability of the device to access the school's network and be mindful of the possibility of potential damage or theft of student's personal gaming devices. Schools should be aware that many of these games

are hosted on platforms such as Discord or Twitch that are not designed for schools and often contain areas, boards, and/or posts that are not school-appropriate. School coordinators should make every effort to limit access to their esports space so that only school members may access the site and that school sites are not accessible by general members of the public.

Club advisors should configure game settings, whenever possible, to reduce or disable violence, gore, or language settings.

Network security, web filtering, and firewall configuration must be reviewed by the AoPTech Senior tech team prior to the start of any esport program. The setup and network configuration process takes both considerable time and planning to ensure the safety of all participants. Each new game added will require additional network/firewall setup and
configuration. Please allow a minimum of three weeks for the AoPTech senior techs to configure and test the school's firewall and network settings prior to deploying the game to the students.

Schools are encouraged to adopt a Code of Conduct for the esports Teams/Clubs based on the Code of Conduct for the Network of Academic and Scholastic Esports Federations (NASEF). To review the NASEF Code of Conduct, please refer to the following links:

- NASEF Code of Conduct (PDF Download)
- Code of Conduct NASEF (Webpage)
- Within their esports code of conduct, schools need to include the following topics:
- In-game chat, game message boards, screen names, and player avatars must be school-appropriate and may not contain language or images that are harmful, defamatory, or otherwise offensive.
- The misuse of school logos is a violation of the RUP, and students and advisors should exercise caution when developing their avatars or team logos.

Policy Violations

Violation of the Responsible Use Policy may result in any or all of the following:
• Loss of use of the school network, computers, and software, including Internet access. The student will be expected to complete work on a non-networked, stand-alone computer system and/or in an offline work environment.
• Issuance of demerits/detentions, if applicable.

• Removal from the esports club or limited from participating in public esports competitions.
• Possible financial obligations for the repair or replacement of damaged school devices.
• Disciplinary action including, but not limited to, dismissal and/or legal

Archdiocese of Philadelphia RUP Policy, Updated 8/2024

To sign the Parental Consent and Student Acknowledgment Form for the 2024-2025 Handbook and all necessary related consents for the current school year, please access our digital signature consent page, go to:

Handbook & Technology Consent E-Signature Page

Or, scan the QR Code with your phone's camera to access our e-signature consent file.

Please read and complete the entire Consent Form and submit it. Thank you.