DREXEL NEUMANN ACADEMY

RESPONSIBLE USE POLICY FOR TECHNOLOGY

Catholic Schools of the Archdiocese of Philadelphia

Revised August 2023

The heart of our curriculum is timeless ~ love, truth, beauty, 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 message for the 48th World Communications Day, Pope Francis said that 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 that is increasingly dependent upon technology, while also 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!

DREXEL NEUMANN ACADEMY

RESPONSIBLE USE POLICY FOR TECHNOLOGY

Catholic Schools of the Archdiocese of Philadelphia

PURPOSE

Technology is a valuable and real-world 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 in chat rooms, cyber bullying awareness and response to ensure an 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. In some cases, outside or personal uses of technology may be applicable under this policy.

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.

N.B. 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.

DREXEL NEUMANN ACADEMY

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 the 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, tease or harass other people.
- **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 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 activity that is illegal under local, state, federal or international law while utilizing AoP-owned resources, computers or networks.

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 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 and could result in copyright infringement claims.

Responsible Use of School Hardware/Devices: All AoP users are responsible for the general care of

School issued hardware/devices. Users must report any damage to the school's hardware/device. 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:

- Teacher school web page, school-issued email and/or phone number
- Teacher created, educationally focused networking sites
- Student Information System and Learning Management System
- Remind Communication app – or similar i.e. Class Dojo, Seesaw

Teachers, administrators or staff members in their normal responsibilities and duties may be required to contact parents outside of the school day. A teacher, administrator or staff member is free to contact parents or guardians using a home phone or a personal cell phone. However, they should not distribute a home phone number or a personal cell phone number to students. 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 should immediately report this to the administrator or appropriate authorities.

Digital Security: Digital security must be at the forefront of every user's mindset. 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-id may also be utilized to protect an account from unauthorized access.

Storage Devices: Use of external removable hard drives, flash 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.

Note - Many of these AI programs require users to be at least 13 years of age for use. Schools should be thorough in their research of the AI programs' Privacy Policy to check for compliance with COPPA, FERPA, and CUPA laws before introducing AI programs for student use. The AoPTech 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/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 personal devices for remote instruction.
- 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.)

Examples of Unacceptable Uses –

Users are not to:

- 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 false information about any persons, students, staff or any other organization.
- Use a photograph, image, video, including-live streaming, or likeness of any student, administrator, employee or volunteer without express permission of that individual and of the principal.
- Create any site, post any photo, image or video of another individual except with express permission of that individual and the principal.
- Attempt to circumvent system security, blocked sites or to bypass software protections.
    - The following activities are strictly prohibited, with no exceptions:
        - 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 or school issued devices must not be disabled or bypassed .
- 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 or school employees
- Harm the goodwill and reputation of the school or system in the community. This includes, but is not limited to: the mis-use of school images and logos, 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 issued device without proper permission and direction.
- Any attempt to alter data, the configuration of a school issued 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 remove covers or protective shells to make repairs to hardware.

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 both student and employee use of school computers and computer accessed content. Due to the evolving nature of technology, the Archdiocese of Philadelphia, Office of Catholic Education reserves the right to amend or supplement this policy at any time without notice.

All school personnel are reminded that all computer, network, and Internet use will be monitored and there is no assurance of privacy or warranty of any kind, either expressed or implied.

Personal Use of Social Media

This section of the policy refers to the personal use of social media sites such as, but not limited to: Facebook, Twitter, YouTube, Instagram, Tumbler, 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 teacher's personal information - such as their personal email address, personal phone number or address.
    - Sharing a fellow student's phone number without their knowledge and consent in order 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 using their first name, last initial. Schools should avoid linking posts to students' personal accounts.

School sponsored organizations must obtain permission from school administration to create any social media accounts related to the organization. Such accounts should be created with a school issued account. Accounts should be maintained and controlled by a minimum of two school appointed adult moderators.

DREXEL NEUMANN ACADEMY

Policy Violations

Inappropriate use in contradiction to the above rules will be addressed by the administration of the school. Violation of these rules 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.
- Possible financial obligations for the repair or replacement of damaged school devices.
- Disciplinary action including, but not limited to, dismissal and/or legal action by the school, civil authorities, or other involved parties.

DREXEL NEUMANN
ACADEMY