Responsible Computing Handbook
Employee Edition

Introduction and Overview

Access to information technologies is integral to the educational mission and purpose of our institution. We utilize technology in nearly every facet of instruction, activity, service, research, and operation of our school. This policy provides expectations for the use of technology as it affects our school and educational community. The school's computer network is provided for limited educational and employment-related purposes, not as a public access service.

Due to the evolutionary nature of technology, it is imperative for faculty and other staff members (hereinafter referred to as employees) to realize that our policies regarding the use of technology in our community will also be evolutionary. We ask all employees to utilize their best judgment when it comes to the use of school technology and keep in mind that our policies related to technology are not meant to supersede our other school policies, but rather to complement them. Although our school provides certain technologies, we recognize that members and guests of our community also have their own technology devices that they bring to our campus and school events. Our policies address the appropriate use of both technologies provided by the school and personally owned technological devices. Please read the policies below before using our network and computers, because by using our technology you agree to be bound by the terms, conditions and regulations below. These policies apply to all employees at all times.

Supervision and Personal Responsibility

All adults utilizing our school campus and our technology are also subject to the terms and conditions of this Technology Use Policy.

All employees must sign an agreement stating that he/she has read and agrees to the terms and conditions in the technology policy **before** they can utilize any school technologies. This agreement must be signed on an annual basis at the beginning of every school year. All employees must sign an agreement stating that he/she has read and agrees to the terms and conditions in the technology policy **before** they can utilize any school technologies. This permission form must be signed annually.

School employees may also use the school technology for personal uses outside of the hours of their obligations as employees, as long as this use does not interfere with job performance or the school's operation of information technologies, financially burden the school or otherwise violate school polices or state and federal laws.

Technology as a Right

All faculty and staff members have a right to utilize the school technology. This policy outlines the best practices associated with use of the school technology. Failure to adhere to this policy may have

possible consequences up to and including termination. Common sense and adherence to the Guiding Principles must prevail.

Our school provides sufficient information technology resources for each employee for regular academic pursuits. If a particular project requires additional resources, the information technology department works with employees on a case by case basis to provide additional resources.

An employee's significant other and children are not permitted to use school technology resources for any reason, unless prior approval is obtained from the employee's supervisor (or the Director of Information Technology).

Privacy

The school reserves the right to monitor and track all behaviors and interactions that take place online or through the use of school technology. All e-mails and messages sent through the school's network or accessed on school owned technology can be inspected. Any files saved onto a school computer or sent through the school network can also be inspected. The school also reserves the right to investigate any reports of inappropriate actions related to any technology used at school.

Filtering

Our school adheres to the requirements set forth by the United States Congress in the Children's Internet Protection Act. This means that all access to the Internet is filtered and monitored. The school cannot monitor every activity, but retains the right to monitor activities that utilize school owned technology. By filtering Internet access, we intend to block offensive, obscene, and inappropriate images and content including pornography.

Right to Update

Since technology is continually evolving, our school reserves the right to change, update, and edit its technology policies at any time in order to continually protect the safety and well-being of our school's community. To this end, the school may add additional rules, restrictions, and guidelines at any time.

Termination of Accounts and Access

Upon termination of your official status as an employee at our institution, you will no longer have access to the school network, files stored on the school network, or your school-provided email account. We recommend saving all personal data stored on school technology to a removable storage device periodically throughout your employment. If you leave our institution in good standing, such as by reason of retirement, we will provide you with email forwarding for a period of 30 days after your termination date.

I. Definitions and Terms Section

Bandwidth – Bandwidth is a measure of the amount of data that can be transmitted in a fixed amount of time.
Cyber-Bullying – Cyber-bullying is when someone sends derogatory or threatening messages and/or images through a technological medium in an effort to ridicule or demean another. Cyber-bullying also takes place when someone purposefully excludes someone else online. For example, a group of students create a group on Facebook that many would like to join, but the student creators purposefully exclude one individual or certain individuals and do not let them join their group. Cyber-bullying also takes place when someone creates a fake account or website criticizing or making fun of another.
Internet – The Internet connects millions of computers together globally, forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet.
Network – The school's network is defined as our computers and electronic devices such as printers, fax machines, scanners, etc. that are connected to each other for the purpose of communication and data sharing.
Technology – Under this policy, technology is a comprehensive term including, but not limited to, all computers, projectors, televisions, DVD players, stereo or sound systems, digital media players, gaming consoles, gaming devices, cell phones, personal digital assistants, CDs, DVDs, camcorders, calculators, scanners, printers, cameras, external and/or portable hard drives, modems, Ethernet cables, servers, wireless cards, routers and the Internet. School technology refers to all technology owned and/or operated by the school.
User – For the purposes of this policy, user is an inclusive term meaning anyone who utilizes or attempts to utilize, whether by hardware and/or software, technology owned by the school. This includes faculty members, staff members, parents, and any visitors to the campus.
Personally Owned Device User – For the purposes of this policy, personally owned device user refers to anyone who utilizes their own technology on property owned or controlled by the school or at a school sponsored event.
PDA – PDA stands for personal digital assistant which is an electronic device which provides some of the functions of a computer, a cell phone, a music player, and a camera.

II. Acceptable Uses Section

User Orientation

All new employees must participate in training about acceptable and unacceptable behaviors related to technology at the faculty orientation. This is required before an employee can utilize any school technologies. Current faculty will participate in ongoing training for social networking.

Purposes and Use Expectations for Technology

Employees may utilize school technologies for some personal/recreational uses, keeping in mind that school technology resources are both shared and finite. These resources include, but are not limited to, disk space, bandwidth, CPU time and effort, printers, faxes, software and workstations. Commercial and recreational use of school technology resources is prohibited. Employees may not utilize school technology to sell, purchase, or barter any products or services. Employees may not resell their network resources to others, including, but not limited to, disk storage space. Employees may not use technology for illegal behavior or behavior counter to the Guiding Principles including, but not limited to, anything contrary to the laws of the State of Pennsylvania. The school is not responsible for any damages, injuries, and claims resulting from violations of responsible use of technology.

Personal Responsibility

We expect our employees to act responsibly and thoughtfully when it comes to using technology. Technology is a finite, shared resource offered by the school to its employees and students. Employees bear the burden of responsibility to inquire with the IT Department or other school administrator when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.

School Provided Technology Resources

Network storage is a finite school resource and we expect employees to be respectful of other users and limit the amount of space and memory taken up on school computers and on the school network. Each employee will be provided a specified quota of storage space to save files on our network based on positional needs. Faculty will be given 10GB, while other administrative employees' allotments may vary.

All employees are provided with a school e-mail account. All e-mails sent from this account are representative of the school and employees should keep in mind school policies regarding appropriate language use, harassment, defamation, and other policies and laws. Employee e-mail accounts are subject to monitoring and have limited privacy. Employees are sharing resources such as bandwidth and server space with others and downloading large files utilizes finite resources. Abusing these resources can result in the loss of this privilege. Please delete old e-mails and save large attachments elsewhere to limit the amount of storage space your e-mail account is using. Each employee is provided with 500 MB of storage space.

This institution has wireless Internet that is protected by a password. Access is only available through Academy owned machines.

Only IT personnel may connect their computers and devices to the school's Ethernet ports and/or disconnect computers and devices currently connected to the school's network.

The school provides individual technology accounts for employees to keep track of their technology use. Users must log off when they are finished using a school computer. Failing to log off may allow others to use your account, and employees are responsible for any activity that occurs through their personal account. An employee is responsible for unauthorized use of his/her technology account, including by children and/or spouses.

International Websites

Because some foreign language websites cannot be filtered using our current system, these websites may only be accessed from school owned technology.

III. Unacceptable Uses of Technology Section

Cell Phones and PDA's

Cell phones and PDA's are permitted on campus, but should only be used in appropriate times and places that do not inhibit the educational process.

Recording, Video, and Photography

Employees are only permitted to send/take photographs or video or live streaming with their phones on school property or at school events that would be in accordance with the Five Guiding Principles.

Web cams are permitted on campus for faculty-directed purposes, but should be used in a safe and appropriate manner. Do not install a web cam onto a computer without permission from the Technology Department.

Employees may only use school authorized resources for recording or data capturing on campus, and then only with specific permission from a school administrator.

Social Networking and Website Usage

Employees may have social networking profiles or accounts, but social networking websites may not be accessed via the school's network unless one's job requires it. Employees who have social networking profiles or accounts may not interact with any current students or their parents or guardians through these profiles/accounts.

Employees may access their own pictures or view other's pictures on photography sharing websites such as Photo Bucket, Webshots, or Flickr.

Do not access material that is offensive, profane, or obscene including pornography and hate literature. Hate literature is anything written with the intention to degrade, intimidate, incite violence, or incite prejudicial action against an individual or a group based on race, ethnicity,

nationality, gender, gender identity, age, religion, sexual orientation, disability, language, political views, socioeconomic class, occupation, or appearance (such as height, weight, and hair color).

Communication: Instant Messaging, E-mail, Posting, Blogs

Employees are not permitted to access from the school's technology any instant messenger services including, but not limited to, AOL, AIM, Yahoo! Messenger, MSN Messenger, and Gtalk.

Inappropriate communication is prohibited in any public messages, private messages, and material posted online by employees. Inappropriate communication includes, but is not limited to the following: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images typed, posted, or spoken by employees; information that could cause damage to an individual or the school community or create the danger of disruption of the academic environment; personal attacks, including prejudicial or discriminatory attacks; harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others; knowingly or recklessly posting false or defamatory information about a person or organization; and communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices. If you are told by another person to stop sending communications, you must stop.

Employees may not utilize any technology to harass, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in our community. This is unacceptable behavior and will not be tolerated. Any behavior, on or off-campus, that is determined to substantially disrupt the safety and/or well-being of the school is subject to disciplinary action.

Do not post or send chain letters or spam. Spamming is sending an unnecessary and unsolicited message to a large group of people. Spamming can occur through e-mails, instant messages, or text messages.

Intellectual Property, Academy Honesty, Personal Integrity and Plagiarism

Do not claim or imply that someone else's work, image, text, music, or video is your own. This is plagiarism and will not be tolerated. Plagiarism is also when you incorporate a piece of someone else's work into your own without giving them appropriate credit. All employees are expected to maintain academic honesty. Do not pretend to be someone else online or use someone else's identity without express permission from that person and/or his/her parent/guardian if he/she is a minor. Do not use, post, or make accessible to others the intellectual property; including, but not limited to text, photographs, and video; of someone other than yourself. This includes intellectual property that you were given permission to use personally, but not publically. This behavior violates school policy as well as state and federal laws.

A work or item is copyrighted when, among other issues, one person or one group owns the exclusive right to reproduce the work or item. Songs, videos, pictures, images, and documents can

all be copyrighted. Copyright infringement is when you violate copyright law and use or reproduce something without the authority to do so. Make sure to appropriately cite all materials used in your work. Do not utilize some else's work without proper permission. As a school professional you have a limited right to use the intellectual property of others within the boundaries of non-profit educational endeavors through Fair Use laws. However, these laws do not afford this privilege outside these limited conditions. Additionally, the schools computers also have software on them that is also protected by copyright law. This software is to be used only in the manner in which the school has the license to use it.

Data and Gaming Devices

Employees may not use school-owned computers to play computer games.

Downloads and File Sharing

Employees may never download, add, or install new programs, software, or hardware onto school-owned computers. Downloading sound and video files onto school-owned computers is also prohibited. This prohibition applies even if the download is saved to a removable hard drive.

Employees may never configure their school computer or personally owned computer to engage in illegal file sharing. The school will cooperate fully with the appropriate authorities should illegal behavior be conducted by employees.

The likelihood of accidentally downloading a virus or spyware when downloading music and movies is very high; therefore employees may not download any sound or video files onto their personally-owned technological devices through the school's technology. Employees also should not download any files or attachments from unknown senders.

Commercial and Political Use

Commercial use of school technology is prohibited. Employees may not use school technology to sell, purchase, or barter any products or services. Employees may not resell their network resources to others, included, but not limited to, disk storage space. The school is not responsible for any damages, injuries, and/or claims resulting from violations of responsible use of technology. Employees who are engaged in fund-raising campaigns for school sponsored events and causes must seek permission from their advisor before using school technology resources to solicit funds for their event.

Political use of school technology is prohibited without prior, specific permission from your supervisor. Employees may not use school technology to campaign for/against, fundraise for, endorse, support, criticize or otherwise be involved with political candidates, campaigns or causes.

Respect for the Privacy of Others and Personal Safety

Our school is a community and as such, community members must respect the privacy of others. Do not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to others. Do not misrepresent or assume the identity of others. Do not re-post information that was sent to you privately without the permission of the person who sent you the information. Do not post private information about another person. Do not use another person's account. If you have been given an account with special privileges, do not use that account outside of the terms with which you were given access to that account.

Be careful when posting private information about yourself online, including your name, your address, your phone number, or other identifying information.

Our institution prides itself on its reputation for excellence; therefore, you may not use the school's name, logo, mascot or other likeness or representation on a non-school website without express permission from our institution. Employees may use the school name on social networking sites in accordance with our Guiding Principles. As a representative of SSA, employees are expected to behave in a respectful and appropriate manner online, as they would in person.

Computer Settings and Computer Labs

Employees are only allowed to alter, change, modify, repair, or reconfigure settings on school-owned computers with the express prior permission of the Technology Department. This includes deleting cookies and history and re-setting the time and/or date on the computer.

Employees are not permitted to alter, change, modify, repair, or reconfigure settings on their own computer or other technology device with the intent to hide unacceptable or illegal use of their own devices. This includes deleting cookies and history and re-setting the time and/or date on the computer.

Purposefully spreading or facilitating the spread of a computer virus or other harmful computer program is prohibited.

Employees may not circumvent any system security measures. The use of websites to tunnel around firewalls and filtering software is expressly prohibited. The use of websites to anonymize the user are also prohibited. The use of websites, both domestic and international, to circumvent any school policy is prohibited. Employees may not alter the settings on a computer in such a way that the virus protection software would be disabled. Employees are not to try to guess passwords. Employees may not simultaneously log in to more than one computer with one account. Employees are not to access any secured files, resources, or administrative areas of the school network without express permission or the proper authority.

No policy can detail all possible examples of unacceptable behavior related to technology use. Our school technology users are expected to understand that the same rules, guidelines, and policies that apply to non-technology related employee behavior also apply to technology-related employee behavior. Our school technology users are expected to use their best judgment when it comes to making decisions related to the use of all technology and the Internet. If there is ever an issue about which you are unsure, ask a supervisor or a member of the Technology Department for assistance.

IV. Response Section

The school's network and other administrators shall have broad authority to interpret and apply these policies. Violators of our technology policies will be provided with notice and opportunity to be heard in the manner set forth in the Employee Handbook, unless an issue is so severe that notice is either not possible or not prudent in the determination of the school administrators. Restrictions may be placed on violator's use of school technologies and privileges related to technology use may be revoked entirely pending any hearing to protect the safety and well-being of our community. Violations may also be subject to discipline of other kinds within the school's discretion. Our school cooperates fully with local, state, and/or federal officials in any investigations related to illegal activities conducted on school property or through school technologies. School authorities have the right to confiscate personally-owned technological devices that are in violation or used in violation of school policies.

If you accidentally access inappropriate information or if someone sends you inappropriate information, you should immediately tell a supervisor or a member of the Technology Department so as to prove that you did not deliberately access inappropriate information.

If you witness someone else either deliberately or accidentally access inappropriate information or use technology in a way that violates this policy, you must report the incident to a supervisor as soon as possible. Failure to do so could result in disciplinary action.

The school retains the right to suspend service, accounts, and access to data, including employee files and any other stored data, without notice to the employee if it is deemed that a threat exists to the integrity of the school network or other safety concern of the school.

V. School Liability

The school cannot and does not guarantee that the functions and services provided by and through our technology will be problem free. The school is not responsible for any damages employees may suffer, including but not limited to, loss of data or interruptions of service. The school is not responsible for the accuracy or the quality of the information obtained through school technologies. (Although the school filters content obtained through school technologies <if you do filter, use this>), the school is not responsible for an employee's exposure to "unacceptable" information nor is the school responsible for misinformation. The school is not responsible for financial obligations arising through the use of school technologies.

VI. General Safety and Security Tips for the use of Technology

Posting Online and Social Networking: Be careful when posting personal information about yourself online. Personal information includes your phone number, address, full name, and other similar information. Remember that anyone might see what you post.

Communications: Think before you send all forms of communication, including emails, IM's, and text messages. Once you send the data it is not retrievable, and those who receive it may make it public or send it along to others, despite your intentions.

Strangers: Do not feel bad about ignoring instant messages or e-mails from unknown people. Save all contacts from known or unknown people who are repeatedly contacting or harassing you. These saved messages will help authorities track, locate, and prosecute cyber-stalkers.

Passwords: Do not share your passwords with others. When creating a password, do not make it anything obvious such as your pet's name or favorite sports team. Also remember to include both letters and numbers in your password if possible.

Downloads and Attachments: Do not open or run files on your computer from unknown or suspect senders and sources. Many viruses and other undesirable consequences can result from opening these items.

Stay Current: Do protect your own computer and devices by keeping antivirus and antispyware up to date. Keep your operating system and application software up to date. Turn off file sharing as an option on your computer.