Westmont Hilltop School District

Policies Governing the Acceptable Use of Technology for School Employees

Introduction and Overview

Access to information technologies is integral to the educational mission and purpose of our school district. We utilize technology in nearly every facet of instruction, activity, service, research, and operation of our schools. This policy provides expectations for the use of technology as it affects our district and educational community. The district'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 district technology and keep in mind that our policies related to technology are not meant to supersede our other district policies, but rather to complement them. Although our district provides certain technologies, we recognize that members and guests of our community also have their own technology devices that they bring to our campuses and district events. Our policies address the appropriate use of both technologies provided by the district 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.

I. Supervision and Personal Responsibility

All adults utilizing our district campuses 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 understands the terms and conditions in the technology policy before they can utilize any district technologies. The sign-off page attached as the last page (Page 7) of this packet must be signed one time only for new hires unless the form is updated in a subsequent year. Employees who are currently on staff are also asked to sign-off that they have read and understand the terms and conditions of the policy.

District employees may use the district technology in the course of their regular job responsibilities. Incidental personal use is permitted as long as it does not affect job performance, occur during instructional time, or interfere with the district's operation of information technologies, and may not financially burden the district or otherwise violate district policies or state and federal laws.

Technology as a Privilege (Not a Right)

The use of district and personally owned technology on district property or at district events is a privilege, not a right. This privilege comes with personal responsibilities, and if you violate the responsible use of any district technologies, your privilege may be revoked and/or suspended.

Our district 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 district technology resources for any reason, unless prior approval is obtained from the administration or the Director of Technology.

Privacy

The district reserves the right to monitor and track all behaviors and interactions that take place online or through the use of technology on our property or at our events. We also reserve the right to investigate any reports of inappropriate actions related to any technology used in the district. All e-mails and messages sent through the district's network or accessed on a district computer can be inspected. Any files saved onto a district computer can also be inspected. Employees have a limited expectation of privacy when using their own technology on district property or at district events so long as no activity violates policy, law and/or compromises the safety and well-being of the school district community.

Filtering

Our district adheres to the requirements set forth by the United States Congress in the Children's Internet Protection Act (CIPA). This means that all access to the Internet is filtered and monitored. The district cannot monitor every activity, but retains the right to monitor activities that utilize district-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 district 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 district's school-aged community. To this end, the district 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 district network, files stored on the district network, or your district-provided email account. We recommend saving all personal data stored on district technology to a removable hard drive periodically throughout your employment. If you leave our district in good standing, such as by reason of retirement, we will provide you with email forwarding for a period of up to 30 days after your termination date.

II. Acceptable Uses Section

User Orientation

All new employees must participate in new employee orientation about acceptable and unacceptable behaviors related to technology before they can utilize any district technologies. This course is only required once.

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 district to its employees and students. Employees bear the burden of responsibility to inquire with the technology department or another district administrator when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.

District-Provided Technology Resources

Network storage is a finite district resource and we expect employees to be respectful of other users and limit the amount of space and memory taken up on district computers and on the district network.

All employees are provided with a district e-mail account. All e-mails sent from this account are representative of the district, and employees should keep in mind district 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.

The school district has wireless Internet that is protected by a password. If you desire to connect your laptop or hand held device to the Internet, you must contact a member of the technology department. Unauthorized access is forbidden.

Only technology department or administrative personnel may connect their computers and devices to the district's Ethernet ports and/or disconnect computers and devices currently connected to the district's network.

The district provides individual technology accounts for employees to keep track of their technology use. Users must log off when they are finished using a district 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.

III. Unacceptable Uses of Technology Section

Social Networking and Website Usage

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

Except for specific pre-approved educational purposes, employees are not permitted to access from the district's technology any instant messenger services.

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.

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, Academic Honesty, Personal Integrity and Plagiarism

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 someone else's work without proper permission. As a professional employee of the district, 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 district's computers also have software on them that is protected by copyright law. This software is to be used only in the manner in which the district or individual school within the district has the license to use it.

Employees may not use district-owned computers to play computer games except for academic purposes.

Downloads and File Sharing

Employees may never download, add, or install new programs, software, or hardware onto district-owned computers without administrative authorization.   Downloading sound and video files onto district-owned computers is also prohibited. This prohibition applies even if the download is saved to a removable hard drive.

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

Commercial, Political, and Personal Use of Technology, including Printers, Copiers, and Fax Machines

Commercial use of district technology is prohibited. Employees may not use district 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 district 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 district-sponsored events and causes must seek permission from the administration before using district technology resources to solicit funds for their event. Likewise, district printers, copiers, and fax machines may not be used for personal or outside organization purposes unless permission is granted by the administration.

The district provides central duplicating services for large print jobs. Building administrators provide specifics regarding the use of office copiers/printers and the use of central duplicating services.

Political use of district technology is prohibited.

Respect for the Privacy of Others and Personal Safety

Other's privacy: Our district 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.

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

Our district prides itself on its reputation for excellence; therefore, you may not use the district's name, logo, mascot or other likeness or representation on a non-district website without express permission from the administration.

Computer Settings and Computer Labs

Employees are only allowed to alter, change, modify, repair, or reconfigure settings on district-owned computers with the express prior permission of the technology department or the administration. 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.

Food and drink are prohibited from district computer labs. Employees may not eat or drink while using any district-owned computers or other technologies.

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 is also prohibited. The use of websites, both domestic and international, to circumvent any district 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 district network without express permission or the proper authority.

No policy can detail all possible examples of unacceptable behavior related to technology use. Our district 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 district 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 an administrator or a member of the technology department for assistance.

IV. Response Section

The district's network administrators and all district 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 and district policy manual, unless an issue is so severe that notice is either not possible or not prudent in the determination of the district administrators. Restrictions may be placed on violator's use of district 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 district's discretion. Our district cooperates fully with local, state, and/or federal officials in any investigations related to illegal activities conducted on district property or through district technologies. District authorities have the right to confiscate personally-owned technological devices that are in violation or used in violation of district policies.

If you accidentally access inappropriate information or if someone sends you inappropriate information, you should immediately tell an administrator or a member of the technology department so as to prove that you did not deliberately access inappropriate information.

The district 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 district network or other safety concern of the district.

V. District Liability

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

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

Westmont Hilltop Employee Acceptable Use Policy Sign-off Page

Your signature on the line below confirms that you have read the Westmont Hilltop School District Employee Acceptable Use Policy and understand the terms and conditions of the policy.

Signature of Employee ____________________________________ Date _______________