The Westmont Hilltop School District

Policies Governing the Student User Agreement (AUP)

MISSION STATEMENT

Unified in a commitment to inspire and to empower resilient, lifelong learners.

Access to information technology 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. We strive to reach the goals of our mission statement and strategic plan by preparing our students for success in the 21st Century. We use the updated National Education Technology Standards (NETS) as a guideline for satisfying technological needs. The new NETS Standards identify several higher-order thinking skills and digital citizenship as critical for students to learn effectively throughout their lifetimes and live productively in our emerging global society. These areas include the ability to demonstrate creativity and innovation, to communicate and collaborate effectively, to conduct research and use information efficiently, to think critically in order to solve problems and make good decisions, and to use technology productively. 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, other school employees, and students to realize that our policies regarding the use of technology in our community will also be evolutionary. We ask all students and 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 technology, 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 school-provided technology and personally owned technological devices. Specifically, we strive to provide district technology opportunities, rights, and responsibilities for students, identify how students as individuals have accessible uses for technology opportunities, resources, and responsibilities, and clearly notify students and parents/guardians of district policies and general safety guidelines for online usage. 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. District Privileges, Responsibilities, and Rights Provided for Students

Supervision and Personal Responsibility

This policy applies only to students. All adult users including teachers, student teachers, faculty members, and staff members have a separate Acceptable Use Policy.

All children and teens visiting our campus are also subject to the terms and conditions of this Student User Agreement.

For the 2019-2020 School Year, ALL students and their parents must sign a permission form **before** they can utilize any school technology.

Following the 2019-2020 School Year, all students and their parents or guardians must sign a permission form in Kindergarten, and annually in grades 7 through 12 (or upon student entry to the school district if newly enrolled) **before** they can utilize any school technology.

Technology as a Privilege (Not a Right)

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

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

Privacy

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

Filtering

Our school 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 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 protect the safety and well-being of our students and community. To this end, the school may add additional rules, restrictions, and guidelines at any time.

Termination of Accounts and Access

Upon graduation or other termination of your official status as a student in our district, you will no longer have access to the school network, files stored on the school network, school-provided email account, or school issued device. Prior to graduation, we recommend that seniors save all personal data stored on school technology to a thumb drive or to an alternate cloud storage account and set up an alternative email account.

II. Student Technology Expectations, Resources, and Responsibilities

Purposes and Use Expectations for Technology

The use of all school-owned technology including the school network and its Internet connection is limited to educational purposes. Educational purposes include classroom activities, career development, communication with experts, and homework. *Commercial and recreational use of school technology resources is prohibited. Students may not utilize school technology to sell, purchase, or barter any products or services. Students may not resell their network resources to others, including, but not limited to, disk storage space. Students may not utilize school technology to play games, visit social networking websites, or send instant messages or e-mails unrelated to the educational purposes stated above. The school is not responsible for any damages, injuries, and claims resulting from violations of responsible use of technology.*

Personal Responsibility

We expect our students to act responsibly and thoughtfully when it comes to using technology. Technology is a finite, shared resource offered by the school to its students. Students bear the burden of responsibility to inquire with Instructional Technology personnel or other school administrators 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 students to be respectful of other users and limit the amount of data stored on school computers and on the school network. Each student has a specified amount of space to save files on our network.

Students in grades 5-12 are provided with a school e-mail account. All e-mails sent from this account are representative of the school and students should keep in mind school policies regarding appropriate language use, bullying, stalking, and other policies and laws. Student e-mail accounts are subject to monitoring and have limited privacy. Students are sharing resources such as bandwidth and network storage 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 Westmont Hilltop School District has wireless Internet capability and access that is protected by a password. If you desire to connect your laptop or hand held device to the Internet, you must utilize the unique ID and password that was assigned to you by the school district. Unauthorized access is forbidden.

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

The school provides individual technology accounts for students 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 students are responsible for any activity that occurs through their personal account.

III. Student Acceptable Uses of Technology

Recording, Video, and Photography

In our efforts to provide a safe and nurturing environment, students are not permitted to send and/or take photographs or video with their phones on school property, school transportation, or at school events. Web cams are not permitted on campus unless issued or authorized by the school district.

Video cameras with audio recording have been installed on all school busses. Video surveillance systems are in place in all district buildings. Exterior cameras have also been installed to monitor activities outside the school buildings when students arrive for the school day and at dismissals. Cameras are also utilized to deter vandalism that might occur beyond the usual school day.

Social Networking and Website Usage

Students may have created social networking profiles or accounts, but social networking websites may not be accessed through the school's technology at any time.

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

Students are not granted unauthorized access to school technology, including any instant messenger services.

Inappropriate communication is prohibited in any public messages, private messages, and material posted online by students. 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 students; 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.

Students may not utilize any technology to harass, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in their community. This is unacceptable student behavior known as cyber-bullying and will not be tolerated. Any cyber-bullying that is determined to disrupt the safety and/or well-being of the school may lead to further investigation, disciplinary action, and/or police referral.

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

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 students are expected to maintain academic honesty. 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 publicly. 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 someone else's work without proper permission.

Downloads and File Sharing

Students may never download, add, or install new programs, software, or hardware onto school-owned computers unless authorized by school personnel and in conjunction with school projects. 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.

Students 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 students.

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

Commercial and Political Use

*Commercial use of school technology is prohibited. Student*s may not use school technology to sell, purchase, or barter any products or services. Students may not resell their network resources to others, including, 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. Students who are engaged in fund-raising campaigns for school sponsored events and causes must seek permission from their advisor before using technology resources to solicit funds for their event.*

*Political use of school technology is prohibited without prior, specific permission from a school administrator or advisor. Student*s may not use school technology to campaign for/against, fundraise for, endorse, support, criticize or otherwise be involved with political candidates or campaigns.

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 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.

Do not voluntarily post private information about yourself online, including your name, your age, your address, your phone number, or other personally identifying information.

Computer Settings and Computer Labs

Students 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 resetting 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. Offenses of this nature may be referred to local police for investigation and prosecution.

Food and drink are prohibited from school computer labs. Students may not eat or drink while using any school-owned computers or other technology.

Students may not circumvent any system security measures. The use of websites to tunnel around firewalls and filtering software is expressly prohibited. Anonymous user websites are also prohibited. The use of websites, both domestic and international, to circumvent any school policy is prohibited. Students may not alter the settings on a computer in such a way that the virus protection software would be disabled. Students are not to try to guess passwords. Students may not simultaneously log in to more than one computer with one account. Students 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 student behavior also apply to technology-related student 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 librarian, teacher, principal, or a member of the Technology Department for assistance.

IV. District Notification to Students

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 WHSD Student Handbooks, 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 a violator's use of school technology 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 while being transported by district-provided vehicles through any school technology. **A violation, which creates a disturbance in the educational process because of connections between what has occurred before/after school hours and the school day, are subject to consequences, including referral to police for investigation. School authorities have the right to confiscate personally owned technological devices that are in violation or used in violation of school policies.**

If you witness someone else either deliberately or accidentally accessing inappropriate information, using technology in a way that violates this policy or vandalizing technology equipment, you must report the incident to a school administrator 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 student files and any other stored data, without notice to the student if it is deemed that a threat exists to the integrity of the school network or other safety concern of the school.

V. District Notification to Parents/Guardians

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 students 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 technology. Although the school filters content obtained through school technology, the school is not responsible for students' 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 technology.

VI. District Reminders for Online Responsibility and Safety

(As stated on Page 3, social networking websites may not be accessed through the school's technology at any time. The information in this section is included for parent/student guidance related to social networking in general.)

Posting Online and Social Networking: Never post personal information about yourself online. Personal information includes your phone number, address, full name, siblings' names, and parents' names. When creating an account on a social networking website, make sure to set your privacy settings so only your friends can view your pictures and your profile. Avoid accepting a friend you do not already know. If possible, set up your account so that you are notified of any postings onto your wall or page. If possible, set up your account so that you have to approve all postings to your wall or page. If possible, set up your account to notify you when someone else has posted and tagged you in a picture. If you have a public profile, be careful about posting anything identifiable such as a sports team number or local park where you spend your free time.

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 and cyber-bullies.
Passwords: Do not share your passwords with your friends. 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.

Please contact your child's building level office if you have any questions regarding this policy before you sign and return the sign-off page that your child received in school. The Elementary School phone number is (814) 255-8707. The Junior-Senior High School phone number is (814) 255-8726.

Please sign and return your child's Student User Agreement sign-off page on the following page and keep the policy for your reference.

Please complete a sign-off page for EVERY child that you have in the district.

This policy was created in partnership with Campus Outreach Services policy resource:
www.CampusOutreachServices.com

Westmont Hilltop School District Student User Agreement Sign-off Page

Your signature on the line below confirms that you have read the Westmont Hilltop School District Student Acceptable Use Policy on the district website and understand the terms and conditions of the policy. You may bring the form to the main office of the school that your child attends or have your child bring the form with him/her.

<u>STUDENT</u>

Student Name (Please Print): ____

Grade Level: _________

Signature of Student: ______________________________________ Date: ___/___/___

<u>PARENT/GUARDIAN</u>

Parent or Guardian Name (Please Print): _______________________________________

Approval for use of Internet and Network Resources

Signature of Parent/Guardian: ________________________________ Date: ___/___/___