USD 417 Morris County
Acceptable Use Policy (AUP)

For the use of Computers, Mobile Devices, Internet Access, Intranet Access, Google Workspace applications, and Internet Applications

Definitions

- User – Refers to anyone, including employees, students, and guests using USD 417 technology, including but not limited to, computers, networks, Internet, email, and other forms of technology services and products.
- Network – This is the wired and wireless technology networks including school and district networks, cellular networks, commercial, community or home-based wireless networks accessible to users.
- Equipment – Any device such as a tablet, smartphone, laptop computer, desktop computer, projector, and iPad, as well as any portable storage devices.
- Software - Any downloaded or physical disc program that is installed on a computer.

Technology provides students with unique and powerful ways to enhance their learning. USD 417 stands behind the use of technology in the classroom to enhance and support learning. We are pleased to be able to offer users access to computer networks and equipment, so they can access district-supplied technology to enhance learning any time of the day.

It is the goal of USD 417 to ensure that each user's interaction with technology contributes positively to the learning environment in school, at home, and in the community. Negative use of technology through USD 417 owned equipment or networks inside or outside of our school that degrades that environment for other users is unacceptable. USD 417 also recognizes that users have widespread access to both technology and the internet; therefore, use of personal devices and connectivity is considered to be included in this Acceptable Use Policy (AUP).

Access to USD 417's network is a privilege, not a right. The use of technology whether owned by USD 417 or devices supplied by the users entail personal responsibility. It is expected that users will comply with USD 417 rules, act in a responsible manner, and will honor the terms and conditions set by policy, administration, and the classroom teacher. Failure to comply with such terms and conditions may result in temporary or permanent loss of access as well as other disciplinary or legal action as necessary. In particular, students will be held accountable for their actions and are encouraged to report any accidental use immediately to their teacher or school administrator.

There is no assumption of privacy while using USD 417's technology or networks. USD 417 reserves the right to monitor user's online activities and access, review, copy and store, or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of USD 417 property, network and/or internet access or files, including email. With the increased usage of software as a service, much of our data is not stored in local servers. This means the servers that store the data that are not on district property.

Google Workspace, Google apps for Education

USD 417 has partnered with Google to offer the entire Google Workspace of applications to each user here at the district. These are free and are able to enhance teaching and learning in the classroom. Every user will be assigned an account, and this will be the district's primary avenue of communication with the user for written communication.

Examples of Google Workspace apps include but are not limited to:

- Calendar
- Classroom
- Drive and Docs
- Gmail
- Google Chat and Hangouts
- Google Meet
- Google Vault
- Google Groups for Business
- Jamboard
- Sites

Terms and Conditions

Listed below are some examples of inappropriate activity on the USD 417 network. USD 417 reserves the right to take immediate action regarding activities that 1) create a security and/or safety issue for the USD 417 network, users, schools or technology resources; 2) expend USD 417 resources on content it determines lacks legitimate education content or purpose; or 3) other activities as determined by USD 417 as inappropriate.

1. Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
2. Criminal activities that can be punished under law.
3. Selling or purchasing illegal items or substances.
4. Obtaining and/or using anonymous email sites, spamming, spreading malware/viruses.
5. Causing harm to others or damage to their property.
6. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
7. Deleting, copying, modifying, or forging other user's names, emails, files or data, discussing one's identity, impersonating other users, sending communications using another user's account, or sending anonymous email.
8. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer malware/viruses or other harmful files or programs, or disrupting any computer system performance.
9. Using any USD 417 computer, device, or equipment to pursue "hacking," internal or external to USD 417, or attempting to access information protected by privacy laws.
10. Accessing, transmitting or downloading large files either for personal use or for the intention of slowing down the network.
11. Using websites, email, networks, equipment, or other technology for political use, personal gain, or a business outside the scope of USD 417 activities; ex: personal business.
12. USD 417 internet and intranet property must not be used for personal benefit.
13. Users must not intentionally access, create, store or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile' or that harasses, insults or attacks others.
14. Advertising, promoting non-USD 417 sites or commercial efforts and events.
15. Users must adhere to all copyright laws.
16. Users are not permitted to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities.
17. Software purchased and used on USD 417 equipment is the property of the district and should not be used for personal gain, installed on personal devices, or copied for other use.
18. Users should not load personally owned software on USD 417 equipment. Doing so assumes the software was a donation to the district and is now the property of USD 417. Any license key, code or information should be surrendered to the USD 417 technology department.
19. Users should not connect to personal hotspots unless specifically allowed by building administration.

Cybersafety and Cyberbullying

All users - Despite every effort for supervision and filters, all users and students' parents/guardians are advised that access to the network may include the potential for access to content inappropriate for school-aged students. Every user must take responsibility for his or her use of the network and make every effort to avoid those types of content. Every user must report security or network problems to a teacher, administrator, or the system administrator.

Personal Safety - When using the network and Internet, users should not reveal personal information such as Name, Home address or city, telephone number, school name, family members names, friend's names or any other identifying information.

Confidentiality of User Information – Personally identifying information concerning students may not be disclosed or used in any way on the Internet without the permission of the student's parent or guardian. Users should never give out private or confidential information about themselves or others on the Internet.

Active Restriction Measures – USD 417 will utilize filtering software, hardware, or other technologies to prevent users from accessing information that is 1) obscene, 2) pornographic, 3) harmful to minors. Attempts to circumvent or "get around" these content filters are strongly prohibited and will be considered a violation of this policy. USD 417 will also monitor online activities of users through direct observation and/or other technological means.

Interactive Web 2.0 Tools

Technology provides opportunities for users to utilize interactive tools and sites on public websites that benefit learning, communication, and social interaction.

Users may be held accountable for the use of and information posted on these sites if it detrimentally affects the welfare of individual users or the governance, climate, or effectiveness of the district. From time to time teachers may recommend and use public interactive sites that, to the best of their knowledge, are legitimate and safe. As the site is "public" and the teacher, school and USD 417 is not in control of it, all users must use their discretion when accessing information, storing, and displaying work on the site. All terms, conditions, and provisions in this AUP also apply to user-owned devices utilizing the USD 417 network.

Student Use of Interactive Web 2.0 Tools

Online communication is critical to the student's learning today, and tools such as blogging, podcasting, and chatting offer an authentic, real-world vehicle for student expression. Student

safety is the primary responsibility of the teachers. Therefore, teachers need to ensure the use of Google Workspace apps, classroom blogs, Student email, podcast projects, email chat features, or other Web interactive tools follow all established Internet safety guidelines including:

- The use of Google Workspace apps, blogs, podcasts or other web 2.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web 2.0 tools. This includes – but is not limited to – profanity, racist, sexist, or discriminatory remarks.
- Students using Google Workspace apps, blogs, podcasts or other web 2.0 tools are expected to act safely by keeping ALL personal information out of their posts or submissions.
- Students should NEVER post personal information on the web, (including – but not limited to – any part of your name, addresses, city, friend's names, or photographs).
- Students should NEVER, under any circumstances, agree to meet someone they have met over the Internet.
- Students should be careful about what they link to during online communication. Before posting a link they must read the entire content of the link to ensure there is nothing negative or otherwise degrading that would go against this or other district policies.
- Students agree not to share their username or password with anyone besides their teachers and parents. Username and password sharing among students is a violation of this AUP. Students should also treat any Web posting spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for these spaces.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in classroom projects and/or be subject to consequences appropriate to misuse.

Student use of Portable Devices

USD 417 has provided some students with Chromebooks for use both in school and away from school. The USD 417-owned devices follow the stipulations outlined in this AUP as well as the District Technology Policies & procedures, and Chromebook Policy.

School Administration and USD 417 Technology staff may search the student device's memory if they feel school rules have been violated. This may include – but is not limited to – audio and video recording, photographs taken on school property that violate the privacy of others, or other issues regarding bullying, etc.

Students may NOT use an audio recording device, video camera, or camera (or any device with one of these, e.g. cell phone, laptop, tablet, etc.) to record media or take photos during school unless they have permission from both a staff member and those whom they are recording. These rules apply to student-owned devices as well. A student-owned mobile device is a non-district supplied device used while at school or during school or district-sponsored activities. The students may use the student-owned mobile devices in class only with the teacher's expressed permission.

Student Supervision and Security

USD 417 does provide content filtering controls for student access to the Internet using District-owned devices on the district network as well as reasonable adult supervision, but at times inappropriate, objectionable, and/or offensive material may circumvent the filter as well as the supervision and be viewed by students. Students are to report the occurrence to their teacher or the nearest supervisor. Students will be held accountable for any deliberate attempt to circumvent USD 417 technology security and supervision.

Students using mobile and cellular devices while at school, during school, or district-sponsored activities are subject to the terms and conditions outlined in this document and are accountable for their use.

Board Approved 1/9/23

Subject to change