Concho Elementary School District #6

Technology Acceptable Use Policy

Updated May 2020

Purpose
The purpose of this Technology Acceptable Use Policy (TAUP) is to clarify the use of District technology resources for the staff and students of Concho Elementary School District #6. This policy applies to all students, staff and others having access to the District network (users). While this policy is NOT intended to prohibit or discourage use of the Internet or resources, it is designed to protect the users and the District against potential liability, security threats and vulnerabilities.

Overview
The District's Technology Acceptable Use Policy is enforced to prevent unauthorized access and activities by online and network users of technology, to prevent unauthorized disclosure or access to sensitive information, and comply with the Children's Internet Protection Act (CIPA). **Users will have no expectation of privacy regarding the use of any technology related resources, including the computer network, Wi-Fi, Internet, email, and telephone.** The District reserves the right to access, view, modify, copy, store, delete and undelete computer and network data and to disclose such information to the appropriate parties.

Acceptable Use

Computers, laptops, and any other end user devices, Wi-Fi, the Internet and other technologies are to be used in a manner that is consistent with the District's standard policies of conduct. The District will verify each academic year that employed staff and matriculated students in the District have a signature both for themselves and from a parent/guardian (for minors) on file acknowledging acceptance of this policy. The TAUP will remain in effect until the end of each academic school year, until the user is no longer a staff member or student of the District, or until privileges have been revoked due to violation of this policy. Please note that the District reserves the right to determine the appropriateness of all information accessed through its technology. The signer of this policy acknowledges and understands that use of District technology shall include but not be limited to the following:

- Users may be subject to limitations imposed on use of any or all technology resources including but not limited to district/school computers, district network and cloud accounts, any end user devices, computer network, Wi-Fi access, inter/intranet, modular audio/visual tools, email, and telephone.
- All classroom use of technology including but not limited to projectors, cameras, document cameras, media cart, that are not physically attached to the building, shall be checked out from the Technology Department at the beginning of the year and back in at the end of the school year.
- Access to websites, email accounts, cloud accounts and other online media will not be used for anything other than District approved communications and learning.
- Computer usage, Internet/Intranet, and email are subject to monitoring and reporting for security and network management.
- Distribution of all information through the District network is subject to scrutiny by the authorized District personnel.
- The District resources are subject to State and Federal laws and illegal use will be dealt with promptly and appropriately.

Unacceptable Use

Computers, laptops, and any other end user devices, Wi-Fi and Internet access are provided as learning resources and curriculum supplements. Access to them is considered a Privilege and not a Right. Violation of this policy will result in disciplinary action, revocation of access to District network, access to District computers, and/or legal action. Examples of inappropriate use of technology include but are not limited to:

- Bringing equipment from home and plugging it into the network without permission from, and a virus check completed by, the Technology Department.
- Attempting to gain access to or download from websites and other media that contain obscene, hateful, extreme violence, pornographic or questionable materials or information.
- Transmitting or posting questionable information or materials using District resources, including District Cloud account resources (Google Apps, etc.) accessed while on or off campus.
- Disclosing sensitive District information without documented authorization.
- Sending sensitive information over District resources without proper encryption and security.
- Soliciting emails that are unrelated to District business and education.
- Using the District network for commercial or financial gain.
- Representing personal views and opinions as those of the District.
- Downloading, installing, or copying software, apps or other files without authorization of the Administration and the Network Administrator.
- Downloading or copying materials or copyrighted information without permission.
- Intentionally using another user's credentials to gain access to his/her files or to use that user's identity for network or online activities.
- Impersonating another user or acting in ANY anonymous fashion.
- Intentionally sharing access credentials with non-authorized individuals.
- Using another person's data or files without permission.
- Copying files, data or programs from the Internet without permission.
- Stealing data, equipment or intellectual property (such as illegally downloading music or video files).
- There will be no use of computer games, unless part of a teacher directed classroom lesson, during school hours (7:00am – 4:30pm).
- Intentionally interfering with normal District operations and activities, including illegal and unauthorized access attempts, propagation of viruses and other malicious software code, or Denial of Service attacks.
- Intentionally damaging technology equipment, files, data or the network.
- Tampering with District computer security systems, applications, documents or equipment. This is considered vandalism, destruction, and defacement of school property.
- Intentionally disrupting the network, or crashing the network and connected systems including Wi-Fi network access and district cloud accounts.
- Attempting to circumvent or sabotage system security measures.
- Using computer programs to decode passwords or to access control information.
- Engaging in any activity that might be harmful to systems, the network, cloud resources or any information stored thereon, such as damaging files or disrupting service.
- Any use of technology deemed inappropriate by District Administrator or representative.
- *Students will be held accountable for completing assignments that require the use of computers even if their in-school computer access privileges are suspended or revoked.*

Special Note – Cyberbullying

Cyberbullying is defined as the use of Internet and/or other technology resources to harass, embarrass, intimidate, hurt, or otherwise demean another individual, group, or entity. Any form of cyberbullying will be dealt with as a punishable breach of the District's conduct policy and will subject the perpetrator to immediate disciplinary action and, if warranted, law enforcement will be contacted. Students in grades 3-8 will be required to participate in a cyberbullying curriculum approved by the District Administrator.

Cyberbullying includes but is not limited to:

- Bullying, harassing, threatening, or humiliating others using email, cloud resources, texting, social networking sites, any type of blog or interest group threads (anything that is/can be accessed by a computer or any end user devices, etc.), website, or telecommunication devices.
- Posting hurtful, negative, threatening, or embarrassing comments on these types of sites or via telecommunication.
- Logging into another person's email account and/or posing as them to harass another person. This is a form of identity theft and is illegal!
- Substantially harass another or others which disrupts the learning environment on or off school property.

Penalties for Inappropriate Use

Misuse of the privilege to use District technology resources may result in possible disciplinary action, revocation of access to network and/or computers, and legal action for any and all users of the network and its resources. This action may include suspension or expulsion for students, dismissal from District employment for staff, and criminal prosecution by law enforcement. Severity of the actions taken by the District and/or government authorities will be based on the severity of the specific infraction(s) at the discretion of the District administration.

Privacy and Administrator's Access to User Files

Since Concho Elementary School District is a public entity all records (excluding those specified by law*****), whether in electronic or hardcopy form, are subject to the Freedom of Information Act and open to public inspection. *Network and cloud storage areas are subject to inspection.* Network administrators may review communications (emails, attachments, files, etc.) to maintain integrity system-wide and ensure that users are using the system in a responsible, acceptable manner. **Users should *NOT* assume that their use of the network or cloud resources are private**. The district reserves the right to monitor network activity in any form that it sees fit to maintain system integrity, and to copy, examine, and delete any files or information on the network or cloud that may suggest that a student/staff member is using school computers systems inappropriately. All inappropriate use will be subject to disciplinary action at the discretion of the District Administrator and consistent with District conduct policy.

*****FERPA*** *(Family Educational Rights & Privacy Act: the federal law that protects the privacy of student education records. This law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.) [20 U.S. C. &1232g; 34 CFR Part 99]*

Information Technology Policy - Hardware, Software, and Data security

1. Responsibility Hierarchy for decisions dealing with hardware, software, and data security:
    - District Administrator
    - District Network Administrator
    - Wilhelm Enterprises
2. Responsibility Hierarchy for directing and supervising the operation of district computer systems:
    - District Administrator
    - District Network Administrator
    - Wilhelm Enterprises
3. Data security, backups, and backup storage will be under the auspices of the Concho Elementary School District. When and if this changes the District Administrator will decide the details of reallocating responsibilities.
4. Access to Intranet locations will be allocated by responsibility through membership in predefined groups. Administration of these groups will be the responsibility of the Network Administrator and/or a member of the Wilhelm Enterprises team with supervision by the District Administrator.
5. AzEDS, student data as stipulated by Arizona Revised Statutes and district level student data will be the responsibility of the Front Office Manager. Assistance on dealing with irregularities in the data will fall to the Network Administrator and/or a member of the Wilhelm Enterprises team.
6. Staff data maintenance will be the responsibility of the District Administrative Assistant unless otherwise authorized by the District Administrator. Assistance in dealing with irregularities in the data will fall to the Network Administrator and/or a member of the Wilhelm Enterprises team.
7. All staff members with access to the district domain will have a unique user name and password. Password changes will be prompted automatically a minimum of three times during the academic year. District Network Administrator will have access to password reset for both domain and cloud accounts (email).
8. Access to personal student and staff information will have an additional layer of password protection over that of entry to the domain.
9. Access to financial records will have an additional layer of password protection over that of entry to the domain.
10. All changes in policy or responsibility for oversight will fall to the District Administrator.
11. Decisions and implementation of this policy and any future changes must be reviewed by the District Administrator for final approval by the School Board

Disclaimer

The District is not responsible for any claims, damages, losses, costs, or other obligations arising from the use of the District network and resources. The District is not responsible for Internet use outside the District network. The District makes no guarantees of the quality of services provided. All charges accrued by a user of the District network are solely the responsibility of the particular user, not the District. All thoughts, views and opinions accessed on the Internet using the District network are NOT the thoughts, views and opinions of the District, its staff or its students, but are understood to be that of the author(s) of such information.

Policy Changes

Changes to this policy during the academic year may be made at the discretion of the district administrator. These will be reviewed at the Technology Committee meeting schedule following the change for inclusion to the TAUP. All accepted changes will be posted to the district website for public viewing.

I have read, understand, and agree to comply with, and abide by the provisions set forth in this Technology Acceptable Use Policy of the Concho Elementary School District #6 (required by all staff and all students) *At the discretion of District administration, students in grade levels pre-K through 2 are not required to sign this agreement.*

Student/Staff Name (print):_____

Signature: _____

Grade/Position: _____

Date: / / 2020

In addition, for students under the age of 18, parent or legal guardian must sign

Parent/Guardian (print): _____

Signature: _____

Date: / / 2020