Corning Union High School District
TECHNOLOGY USE AGREEMENT (EMPLOYEES)

The Technology Department shall maintain an accurate registry of the inventory of all computer equipment.

- No hardwired computer equipment or other technology specifically designated to a room shall be removed from District premises except to the District Office or other school site for presentation purposes, and only after contacting the Technology Department for approval. Employee desks, where cabled technology is located/sitting/used, may not be moved without Site Principal and Technology Director approval. This also includes minor changes such as moving a computer to the next room.
- Mobile computing devices may be shared, moved between assigned classrooms. Employee-issued mobile computing devices may be taken off-site as needed for approved district business.
- No donations of computer equipment shall be accepted without the approval of the Technology Director, nor may old equipment be disposed of without such permission.
- No computer hardware or networking devices, such as wireless access points, shall be connected to the District network.
- Users are aware and agree that all technology and anything on company equipment is company property and subject to review, monitoring, and inspection by the company at any time, with or without notice, and without the user's prior consent. This includes, but is not limited to, all files, data, communications (including email and instant messages), internet Browse history, and software.
- Users should have no expectation of privacy when using company-provided equipment or systems, including personal content or communications stored or transmitted on them. This policy applies to all company-owned or leased devices, networks, applications, and services, regardless of where or when they are accessed.
- Computer hardware or software can become obsolete, or no longer capable of performing a job or education-related task. If the hardware or software is replaced with new hardware or software, the obsolete computer or software will no longer be supported by the District’s Technology Department. However, the replacement computer or software will be fully supported.
- Users shall contact the Technology Department for approval of any network infrastructure requests (installation of wiring) before purchasing computer equipment that will require additional infrastructure (connections to the local area network).
- Users shall not attempt to gain unauthorized access to the District system or to any other computer system through the District system, or go beyond their authorized access. This includes attempting to log in through another person’s account or accessing another person’s files.
- Users shall avoid the inadvertent spread of computer viruses by following safe computing practices.
- Users shall not make deliberate attempts to disrupt the computer system's performance or destroy data by spreading computer viruses or by any other means.

- Vandalism will result in the cancellation of user privileges and disciplinary action. Vandalism includes uploading, downloading, or creating computer viruses, and/or any malicious attempt to harm or destroy district equipment or materials or the data of any other user, including so-called “hacking.”
- Employees shall not access, post, submit, publish or display harmful or inappropriate matter that is threatening, obscene, disruptive, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion or political beliefs. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access to his/her supervisor. This will protect users against an allegation that they have intentionally violated the Acceptable Use of Technology Policy/Procedure.
- Users shall not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
- Employees shall not use the system to promote unethical practices or any activity prohibited by law, board policy, or administrative regulation.
- Employees shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or forge other users' email.
- Employees shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee.
- Employees shall not engage in any data mining activities using district-issued devices or networks.
- Users shall respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. Copyrighted material shall not be placed on the system or network resources without the author’s permission. Employees may download copyrighted material only in accordance with applicable copyright laws. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether they can use a work, they must request permission from the copyright owner. Media such as audio or video CDs or DVDs may not be copied to the local computer or network resources.
- Employees shall not develop any classroom or work-related websites, blogs, forums, or similar online communications representing the District or using district equipment or resources without permission from the Superintendent or designee. Such sites shall be subject to rules and guidelines established for district online publishing activities, including, but not limited to, ADA compliance, copyright laws, privacy rights, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs, any such site shall include a disclaimer that the District is not responsible for the content of the messages. the District retains the right to delete material on any such online communications.
- Users are responsible for the use of their individual account(s) and shall take all reasonable precautions to prevent others from being able to use their account. Employees shall keep account information, home addresses, and telephone numbers private. Users shall not provide their password to another person or post their password

in any place, except those passwords that shall be provided to the Superintendent or designee.

- Users shall immediately notify the system administrator and/or site principal if they have identified a possible security problem. Users will not search for security problems, because this may be construed as an illegal attempt to gain access.
- Users shall not post information that, if acted upon, could cause damage or a danger of disruption.
- Users shall not engage in personal attacks, including sending prejudicial or discriminatory emails.
- Users shall not harass another person. Harassment is persistently acting in a manner that is intended to distress or annoy another person. If a user is told by a person to stop sending messages to them, they must stop.
- Users shall not post false or defamatory information about a person or organization.
- Users shall use the system primarily for educational and professional or career development activities, and limited personal research and exploration activities. Personal use is limited to personal time. All of the restrictions set forth in this regulation apply to personal as well as business use.
- Users shall not download large files unless absolutely necessary. Large downloaded files should be immediately erased from shared resources.
- Users shall not post chain letters or engage in “spamming.” Spamming is sending an annoying or unnecessary message either individually to a large number of people or by using the District’s group email accounts.
- Users shall check their email frequently and delete unwanted messages promptly.
- Users shall not make changes to computers or other network resources. This includes the installation of any computer programs, hardware, or anything that affects the operating system. Users shall not alter any system settings or system network configurations. Users shall not alter internet browser settings, including the installation of add-ons or toolbars.
- Software and hardware shall not be purchased by the user. All purchases must be requested through the Technology Department, and a requisition process will be followed.
- All installations of software and hardware shall be completed through the Technology Department upon determination that the software/hardware is necessary and will meet intended educational needs.

_____ _____

Printed Name Signature

_____

Date