



Personnel AR 4040 Employee Use of Technology: Staff Acceptable Use Policy (AUP)

West Contra Costa Unified School District strongly believes in the educational value of technology and the internet. In this connected world, staff have access to tools that enable them to effectively communicate, collaborate, and create. Technology access in the district supports and enhances learning and teaching. The West Contra Costa USD network and technology equipment are to be used in a responsible, efficient, ethical, and legal manner. WCCUSD provides email to all full or part time employees of the district. WCCUSD recognizes that email is a valuable communication tool that is widely used across our society. Staff members are provided with district email accounts to improve the efficiency and effectiveness of communication both within the organization and with the broader community. Staff are expected to be good citizens of the district network and technology.

Educational technology and tools are becoming more prevalent and accessible to educators and students. Requests to utilize specific educational technology and tools may originate from students, parents, other staff, or directly from the provider of educational technology services. Staff members are reminded that the district has a software approval process to ensure that all software has been vetted to maintain student and staff privacy as required under COPPA and other applicable state and federal laws. Use of educational technology that has not been preapproved by the district is **UNACCEPTABLE** and intentional or inadvertent disclosures of personal information may result in disciplinary action. When and where applicable, law enforcement agencies may be involved.

Acceptable uses of the network and technology that support learning and teaching include:

- Log on to your own account to use the Internet
- Log off your computer any time you are stepping away from your computer.
- Notify building or district technology staff if you encounter inappropriate materials or sites at helpdesk.wccusd.net
- Report any security problems immediately to helpdesk.wccusd.net
- Keep passwords private.
- Take all reasonable precautions to protect access to your account.
- Be cautious of suspicious links and report anything to helpdesk.wccusd.net that concerns you.
- Practice printing conservation.
- Protect the privacy of staff and students.
- Observe copyright guidelines and fair use policies.
- Follow all district policies and local, state, and federal laws.
- Read and be familiar with the student Acceptable Use Policy (AUP) and notify a site administrator or district personnel if a student violates the AUP.

Unacceptable Use of Technology that does not support teaching and learning include:

- Leaving programs accessible to others such as allowing students to use staff devices or logins.
- Accessing or viewing obscene, profane or objectionable materials or sites.
- Accessing sites that promote any illegal activity.
- Using the network for financial gain (i.e. auctions, eBay or gambling).
- Personal use during scheduled work time.

- Downloading content without proper licensing and approval.
- Trespassing in folders, files, devices, or accounts other than those you have been preauthorized to access.
- Engaging in practices that threaten the network (e.g., opening non-requested or suspicious attachments or links).
- Changing network and security settings on school computers.

Computer Trespassing and Unauthorized Uses

A person who knowingly or intentionally accesses or exceeds authorized access to a district computer system, a district computer network, or any part of a computer system or computer network without the consent of the owner of the computer system or computer network, or the consent of the owner's licensee, commits computer trespass, a Class A misdemeanor, under California Penal Code section 502.

The West Contra Costa Unified School District has attempted to provide a safe network environment. Staff are advised that using the district's system might provide access to information that contains inaccurate or objectionable material. **Accessing information on the Internet is ultimately the responsibility of the user.** The district prohibits the use of obscene or other objectionable materials. In addition, staff should be aware of the following:

- By authorizing use of technology resources, the District does not relinquish control over materials on the systems or contained in files on the systems. Files stored on school based computers and communications via email, Internet browsers, or voice mail are not private.
- Electronic messages and files stored on school-based computers or network systems may be treated like any other school property. Administrators, staff, or network personnel may review files and messages to maintain system integrity and, if necessary, to ensure that users are acting responsibly.
- School district employees should be aware that data and other material and files maintained on the school district system may be subject to review, disclosure, or discovery. The school district will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.
- Connecting a personal device to a district computer can result in sharing of personal information from one device to another.
- Teachers will instruct students in the proper use of the Internet and the district network and will guide them toward appropriate materials. Outside of school, families bear the same responsibility. It is a shared responsibility of district staff and parents/guardians to supervise student access to Internet content, and it is the student's responsibility to avoid accessing such material.

Use of Artificial Intelligence

Artificial Intelligence (AI) is a system of machine learning that is capable of performing complex and original tasks such as problem solving, learning, reasoning, understanding natural language, and recognizing patterns in data. AI is becoming more prevalent in our daily lives and is being integrated in a variety of technical applications. The District recognizes that the use of AI can enhance student learning experiences and be a resource for staff and teachers. The District authorizes the ethical and legal use of AI as a tool to support and expand on classroom instruction, increase learning opportunities, and as a general tool for staff and teachers subject to limitations listed within this policy and any other applicable Board Policies.

The District may consider whether the adoption of a particular AI tool may have a significant impact on the terms and conditions of employment for its staff, such that the District may be obligated to negotiate the effects with a collective bargaining unit.

The District has developed the following guidelines and protocols for employee use of AI:

1. Before allowing students to use a specific AI platform in the classroom and before using an AI tool as a resource, employees should ensure that the AI system has been vetted and approved by the District software approval process and therefore has a CA Student Data Privacy Agreement, or otherwise meets the District's safety standards.

2. When applicable, the District or its staff should attain parental consent before offering certain AI services to students.
3. Evaluation of an AI tool may include whether it is an open or closed environment for purposes of data collection, whether it meets current student data privacy standards, whether it can be offered in an equitable manner, whether any inherent bias can be minimized or eliminated, and that safeguards are in place to confirm that accurate and factually correct information can be provided.
4. Teachers shall clarify whether or to what extent students are prohibited from using AI on an assignment.
5. Employees must be cognizant of the information they are sharing with any open AI system and shall not share any confidential information or personally identifiable information of another student, employee, or other person. Personally identifiable information (PII) includes, but is not limited to, a person's name, address, email address, telephone number, Social Security number, or other similar personally identifiable information. Confidential information includes, but is not limited to, information in a student's education record such as their grades and information pertaining to an Individualized Education Plan.

Abuse of the technology may result in:

- Suspension or cancellation of use or access privileges.
- Payments for damages or repairs.
- Discipline under appropriate school district policies including suspension, expulsion, exclusion or termination of employment, or civil or criminal liability under applicable laws.

If you are issued district technology (laptop, desktop, cell phone, etc) you are responsible for following the procedures outlined in the Stolen Device Reporting procedure (linked and available at helpdesk.wccusd.net). Upon leaving WCCUSD, you are responsible for returning your device(s) to your supervisor or to IT Services. District-issued devices are not transferable, meaning that devices cannot be given to anyone other than the assigned staff member.

ACKNOWLEDGEMENT OF ACCEPTABLE USE POLICY

Users must acknowledge their understanding of this policy by submitting a signed staff AUP Form annually. Failure to adhere to this policy and its regulations may result in suspension or cancellation of user privileges and may result in disciplinary action up to dismissal. District Due Process procedures will apply.

I have read and understand the WCCUSD Staff Acceptable Use Policy.

Printed Employee Name: _____

Work Site: _____

Employee Signature: _____ Date: _____

Updated: July 2024