

Student Acceptable Use Agreement 2023-24

BOARD POLICY:

USD 345 is committed to making advanced technology and increased access to learning opportunities available to all students. The goal of the district in providing access to students is to promote educational excellence in schools by facilitating resource sharing, innovation, and communications. The use of computers, tablets, networks, email, the Internet, or other online services shall be in support of education and research consistent with the district's educational objectives.

Administrative Implemental Procedures:

1. Student Responsibilities: Regardless of any “technology protection measure” implemented by the District as may be required by the Children’s Internet Protection Act, students are responsible for good behavior on computers, tablets, networks, email, the Internet, or other online services just as they are in a classroom or a school hallway. General school rules for behavior and communications apply. Network storage areas will be treated like school lockers. Network administrators, teachers, and other appropriate district staff may review student files and student communications from time to time to prevent misuse and to ensure students are using the system responsibly and in compliance with laws and district policies. Communications on the network are often public in nature; students should not expect that files stored on district servers will be private.
2. Permission: Students shall not be allowed to utilize electronic communications prior to accepting the terms of the Student Acceptable Use Agreement. To remain eligible as users, students' use must be consistent with the educational objectives of the district. Access is a privilege, not a right, and inappropriate use will result in, among other disciplinary measures, the cancellation of those privileges. Students will display school-appropriate conduct when using the computer equipment or network and shall maintain an environment conducive to learning.
3. Violations: Administrators, teachers, and other appropriate district employees will decide what is inappropriate use. Violating this policy may result in:
 - a. Restriction or loss of network/technology access; and/or
 - b. Disciplinary or legal action including, but not limited to, suspension or expulsion from school and/or criminal prosecution under appropriate local, state, and federal laws; and
 - c. Assessment of the cost of damages to hardware/software.
4. Inappropriate Use: The following uses of school-provided computers, tablets, networks, email, the Internet, or other online services are not permitted on the part of USD 345 students:
 - a. Accessing, uploading, downloading, or distributing pornographic, obscene, or sexually explicit material
 - b. Transmitting obscene, abusive, sexually explicit, or threatening language
 - c. Violating any local, state, or federal statute
 - d. Accessing another individual's materials, information, or files without permission
 - e. Violating copyright or otherwise using the intellectual property of another individual or organization without permission
 - f. Using others' login credentials (username/password)
 - g. Vandalizing, defined as any unauthorized access and/or malicious attempt to damage computer hardware/software or networks or destroying the data of another user, including creating, uploading, or intentionally introducing viruses
 - h. Intentionally wasting limited resources
 - i. Using district resources for commercial purposes
 - j. Cyberbullying, Harassing, insulting, or attacking others
 - k. Using, disclosing, or disseminating personal information online such as full name, home address, phone number, etc., except with approval by certified or administrative district staff
 - l. Using e-mail lists from the district's Internet site, network, or servers to create mailing lists

- for non-school purposes
- m. Gaining unauthorized access to resources or entities
 - n. Invading the privacy of individuals
 - o. Improperly altering the set up of computers as determined by the network administrator
 - p. Failing to follow a district policy while using computers or failing to follow any other policies or guidelines established by district administration, teachers, or other appropriate district staff
 - q. Seeking to gain or gaining unauthorized access to information resources or other computing devices
5. Security Risk: Any student identified as a security risk or having a history of problems with other computer systems may be denied access.
 6. Disclaimer: The district makes no warranties of any kind, whether express or implied, for the access it is providing. The district will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence or user errors or omissions. Use of any information obtained via the Internet is at the user's risk. The district denies any responsibility for the accuracy or quality of information, or for any commercial transactions conducted through its system.
 7. Statements of Personal Belief: Any statement of personal belief found on computers, tablets, networks, email, the Internet, other online services, or other telecommunication system is implicitly understood to be representative of the author's individual point of view, and not that of USD 345, its employees, or the participating school. No representations to the contrary shall be published without written approval from the district. Principals or district administrators may review all content in any Internet or online accounts paid for, in whole or in part, by the district or any school, without notice of any kind.
 8. Accepted and Signed AUA: Prior to use of school computers or networks, (e.g. the Internet or other online services), each student shall electronically accept and sign this Acceptable Use Agreement (AUA) during the annual online enrollment process. If a student is under the age of 18, a parent/guardian shall also sign the contract(s). The AUA must be electronically accepted and signed each school year. BOE Policy applies to all students regardless of whether they have submitted a signed AUA. If a student has not accepted and signed the AUA as required above, access to computer services and accounts is prohibited.