

## **Acceptable Use Policy (AUP) for Information Services – Student/Parent Edition 2019-2020**

All USD 460 students and their parent/guardian shall annually pledge compliance with the AUP prior to using the district's Information Services. For this policy, Information Services is defined as any interaction between a student or parent/guardian and the district's computer network. This includes, but is not limited to, usage of school/district-owned computers and tech devices, services such as Infinite Campus, and access to the Internet.

**Please read this document carefully.** When attested by the student and his or her parent or guardian on the Parent/Student Authorizations form, this document becomes a binding consent agreement. Listed below are the provisions of this agreement. If any user willfully violates any of these provisions, access to Information Services will be denied until such time that the alleged violation can be resolved. Violators may be subject to disciplinary action, up to and including expulsion from school, and legal action by law enforcement.

Attestations will remain on file. A new attestation is required each school year.

The goal in providing these Information Services is to provide students with access to appropriate educational information. USD 460 will take reasonable and lawful precautions to protect the privacy of students from potential misuse or abuse. All users must be continuously on guard to avoid inappropriate and illegal interaction with any information system.

### **TERMS AND CONDITIONS OF THIS AGREEMENT**

**1. PERSONAL RESPONSIBILITY:** Users are fully responsible for their use of the district's Information Services. If any user is suspected of violating this AUP, the district will investigate the situation and, where appropriate, cooperate with law enforcement if a criminal violation is suspected.

Each user shall accept personal responsibility for reporting any misuse of Information Services to the building principal or the technology supervisor. Misuse can come in many forms, but it is commonly viewed as any transmission that indicates or suggests pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other issues described below. The Board of Education reserves the right to modify and update the AUP at any time.

**2. ACCEPTABLE USE:** Any student use of Information Services must be in support of an approved district goal, objective, local or state standard, and/or approved lesson plan. All research shall address a specific educational goal and/or objective of USD 460. Use beyond these limits is authorized only when the student is under the direct supervision of a district employee. The AUP requires all users to comply with all applicable laws and board of education regulations, but is not limited to matters of law. The district will monitor usage of its Information Services to ensure compliance with federal, state and local laws and/or this AUP. The district will investigate possible violations when information warrants. All complaints or concerns regarding possible AUP violations should be directed to your building principal or the technology supervisor.

### **Unacceptable Uses of Internet/Intranet Services**

In addition to use of Information Services for any illegal purposes (some of which are described below), it is a violation of the AUP to:

- Post, distribute or disseminate another's intellectual property or proprietary information, including trade secrets or copyright information, without specific authorization of the rights holder. Pursuant to the Digital Millennium Copyright Act, accounts of users who repeatedly infringe on the copyrights of others will be terminated.
- Transmit, post, store, or knowingly receive any material that is obscene, sexist, racist, or constitutes child pornography under current law and specifically the 2000 Children's Internet Protection Act.
- Access or attempt to access depictions of obscenity, child pornography, adult content, sexuality issues, profanity, nudity, and material deemed "harmful to minors" in any form.
- Use electronic mail other than the USD 460 address, chat rooms, and other forms of direct electronic communications without proper authorization.
- Engage in unauthorized access, hacking, and other unlawful activity.
- Disclose, use, or disseminate personal information regarding adults or minors without proper authorization.
- Threaten bodily harm, destruction of property, or otherwise engage in harassment. Access or attempt to access sites that promote intolerance/extremism, weapons/bombs, and violence, or, are tasteless in nature.

- Access or attempt to access sites that engage in gambling or conduct online auctions.
- Transmit or post any defamatory information, unethical or illegal solicitation, or use of inappropriate language, such as profane or language inciting violence.
- Use network resources in excess of any prescribed limits on bandwidth or disk storage/utilization.
- Obtain, or attempt to obtain, unauthorized access to, monitor, or use any data, systems, or networks without the expressed permission of the owner.
- Disclose your password(s) for accessing Information Services to another party, or otherwise facilitate unauthorized access.

Users are fully responsible for their use of the district's Information Services. If any user is suspected of violating this AUP, the district may, among other things, investigate the situation and, where appropriate, cooperate with law enforcement if a criminal violation is suspected.

**3. PRIVILEGES:** The use of the Internet and school Information Services is a privilege, not a right, and inappropriate use may result in the cancellation of this privilege. The primary use of the Internet and school information system is for school-related purposes. Users shall have no expectation of privacy when using district e-mail or other official communication systems. Use of any school supplied facility or equipment is subject to unannounced monitoring and review by the district at its discretion. School management may access and read user Internet messages or review Internet sites visited by users at any time. Using this account in support of illegal activities is prohibited. District administrators, operating under the auspices of the USD 460 Board of Education, will decide what is appropriate use, and their decision is final. At any time deemed necessary, the district administration may request that the system administrator deny, revoke, or suspend specific user accounts.

**4. SERVICES:** USD 460 makes no warranties of any kind, whether expressed or implied, for the service it is providing. USD 460 will not be responsible for any damages you suffer while on this system. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries, service interruptions caused by the system, or your errors or omissions. Use of any information obtained via the information system is at your own risk. USD 460 specifically denies any responsibility for the accuracy of information obtained through its services.

**5. SECURITY:** If you identify a security problem, notify the technology supervisor at once. Never demonstrate the problem to other users. Never use another individual's account. Any user identified as a security risk will be denied access to Information Services.

**6. VANDALISM:** Vandalism is defined as any malicious or willful attempt to harm or destroy data of another user, agency, or network that is connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, unauthorized downloading and/or installation of software, plug-ins, patches, and/or storage of audio or video files. Vandalism may result in the loss of computer services, disciplinary action, and legal referral.

### **General Rules and Guidelines**

Students using computers and/or other tech devices in USD 460 shall observe the following:

1. The student will demonstrate appropriate knowledge and understanding of computer/device use.
2. Students will not tamper with another student's work or with the computer system.
3. Students will use their district USD 460 e-mail address ONLY during school hours.  
Involvement in chat lines will only be allowed for class purposes and will be supervised by a teacher.
4. Students are not to download applications.
5. Students wishing to install additional software from an outside source and use it in the school's computer system must have a teacher complete an "Additional Technology Request" form on the student's behalf and send it to the technology supervisor.
6. Students are to use computers and tech devices for educational purposes. Students wishing to complete classroom assignments have priority for computer/device usage.