USD 408
Computer/Internet Acceptable Use Policy (AUP) and Internet Safety Policy
Students

Computers and internet access are provided to USD 408 students to enhance instruction and learning via technological resources. Students are expected to use computers/internet as educational resources and in a manner which is responsible, legal, and appropriate. A student's failure to adhere to the Acceptable Use Policy will result in the revocation of the student's access privileges.

Each parent/guardian has the right to choose whether or not his student has internet access. The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

Responsible users of the school network/internet:

- Understand that NONE of their communications and information accessed via the network is considered private or confidential. USD #408 reserves the right to access all user accounts at any time.
- Understand that network/internet usage must be in support of education and research, consistent with the purposes of USD #408.
- Understand that they should not reveal their full name, phone number, or give out their home addresses in any communications over the internet.
- Completely understand the Acceptable Use Policy before logging on.
    - Understand that if the Acceptable Use Policy is violated, the student's access to internet can be denied, his account on the school network can be revoked, and the district also has the right to appropriately discipline the student.
    - If a student is removed from the network, he has the right to appeal that removal in writing to the principal within (10) days. The principal's decision will be final.
    - Once removed from the network, there is no obligation to provide a subsequent opportunity to access the network again.

Improper Use

Uses of the network which are prohibited, but are not limited to:

- Use of the network for or in support of any illegal purpose (K.S.A. 21-3755)
- Purposefully send, receive, and/or view obscene, pornographic, or sexually explicit material
- Any violation of students' rights to privacy and the confidential maintenance of certain information (i.e.: students' grades or test scores)
- Use of chat rooms
- Use of profanity, obscenity, or language that is generally considered offensive or threatening to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities—harassment of any nature will not be tolerated.
- Copying commercial software in violation of state, federal, or international copyright laws
- Use the internet for financial gain or for the transaction of any business or commercial activities
- Plagiarizing (claiming another person's writing/work as your own) any information accessed via the network or the internet
- Use of the school network for political lobbying
- Intentionally disrupting the use of the network for other users, including but not limited to the use of any process, program, or tool for ascertaining passwords or engaging in "hacking" of any kind which includes but is not limited to the illegal or unlawful entry into an electronic system to gain secret information
- Providing access to the school network to unauthorized individuals
- Use the network to violate any provision of the school discipline code
- Knowingly spread computer viruses
- Utilize computer data (i.e. other student's work product or a teacher's test) without authorization to gain an improper academic advantage
- Join a listserve.
- Play games or pursue other non-academic purposes without permission

- Modify, damage, destroy, or copy any data to which they are not authorized.
- Destroy, modify, or abuse network hardware or software.

Levels of Violations

1. No Violation (no discipline suggested)
   A. A student accidentally comes in contact with an inappropriate site. The student backs out immediately and informs the teacher.
   B. A legitimate site comes up as a blocked site.
2. Minor Violation (non-suspendable offenses)
   A. A student is deliberately searching for restricted and/or inappropriate material.
   B. Any violations of the student code of conduct and/or school district policy at this level.
3. Intermediate Violation (suspendable offenses)
   A. A repeat offense of a minor violation.
   B. Sharing login or password information.
   C. Use of proxy servers or circumvention of network protection to download games, music, videos, etc.
   D. Any violations of the student code of conduct and/or school district policy at this level.
   E. Modification of computer settings and/or applications
4. Serious Violation (suspendable and/or prosecutable offenses)
   A. A repeat offense of an Intermediate Violation
   B. Theft of login or password information
   C. Theft of data or material
   D. Damage to the computer systems, software, network, etc.
   E. Intentionally disrupting the network or crashing the network
   F. Unauthorized access to network systems and/or data
   G. Using the computers and/or network for illegal activities
   H. Any violations of the student code of conduct and/or school district policy at this level.

Violation of Policy & Possible Consequences for Violations

Any student who violates this policy shall be subject to any of the disciplinary actions listed below. Additionally, if student conduct constitutes a violation of copyright laws or Kansas Statute 21-3755, the student may be subject to prosecution under such laws. Any student who intentionally damages or destroys district hardware and/or software, either directly or indirectly shall be responsible for all costs associated with repair and/or replacement of parts and services.

1. Warning
2. Suspension of Internet privileges
3. Suspension of computer privileges
4. Detention/Saturday school
5. School Suspension
6. Removal from computer program (class or lab)
7. Expulsion
8. Prosecution
9. Restitution

These guidelines may change from time-to-time as technology, laws, and society evolves.

Disclaimers

USD #408 makes no warranties of any kind, whether expressed or implied, for the service that it is providing. The district will not be responsible for any damages a user suffers which may include the loss of data resulting from delays, no-deliveries, mis-deliveries, or service interruptions caused by the district's negligence or by the user's errors or omissions. Use of any information obtained via the internet is at the user's own risk. The district is not responsible for the accuracy or quality of the information obtained through its services. All users need to consider the source of any information they obtain and consider how valid that information may be.

Users may encounter material which is controversial and which users, parents, teachers, or an administrator may consider inappropriate or offensive. However, on a global network, it is impossible to effectively control the content of data and users may discover controversial material. The district will provide monitoring and filtering services in an attempt to block access to indecent material; however, it is the user's responsibility not to initiate access to such material.

USD 408
Computer/Internet Acceptable Use Policy (AUP) and Internet Safety Policy
Parent/Student Contract

Students must assume the following responsibilities:

1. Students are to treat all equipment with care and to report instances of abuse or misuse as soon as the student becomes aware of it. Students are expected to report any malfunction or problem immediately upon discovery to the teacher, lab aide or district technology coordinator.

2. Students are prohibited from sharing their computer passwords. Passwords are to be kept confidential.

3. Students are not to allow other individuals to access or update information under their user name/password. Students will be held accountable for all computer activity performed under their log in and password.

4. The student and/or the guardian is responsible to pay all repairs and/or replacement cost if the student vandalizes or otherwise intentionally damages any district hardware or software. By signing this contract, the student and the guardian expressly agree to be responsible for the payment of any costs incurred. In such cases, the student will be referred to the building administrator for appropriate discipline.

5. A student who damages, destroys, or copies another student's data will also be referred to the building administrator for appropriate disciplinary action. Incidents in which a student copies another student's data will be treated as cheating.

6. Students are not to tamper or attempt to gain access to computer data for which they do not have authorization. Such an act will be considered equivalent to tampering with a teacher's written records or attempting to gain access to confidential student information.

7. Students may not load or copy unauthorized software onto district computers.

8. Students will follow the internet acceptable use policy and Internet Safety Policy delineated in the previous pages.

Any student who disregards these responsibilities will be considered in violation of the USD 408 Computer/Internet Acceptable Use Policy and Internet Safety Policy. In addition to violating school policy, students may also be subject to prosecution under the copyright laws of the USA and/or Kansas Statute 21-3755.

Acknowledgement

I ACKNOWLEDGE THAT I HAVE READ AND UNDERSTAND the Computer/Internet Acceptable Use Policy (AUP) and Internet Safety Policy.

As the parent/guardian of a minor student, I give permission for my student to access the internet at school.

Check One: Yes _____ No _____

Student's Name (Please print) _____ Birth Date: _____

Student's Signature _____ Date: _____

Parent/Guardian's Signature _____ Date: _____

Student Grade Level _____

PLEASE NOTE: If you already have a Computer/Internet account with USD 408, your password will not be changed, unless you provide a new password. If you are new to USD 408 or would like your password changed, please provide a student password to be used for Computer/Internet access: _____