Student Acceptable Use Policy
For Network Access and Internet Safety

Introduction

The Burrton School District provides access to shared resources on the school's network for students to use for class-related work. Burrton Schools also provides access to the Internet and the web for research and other educational uses. These resources are available to all students for use related to classroom work. It is a privilege to access these resources. This privilege may be revoked at any time at the discretion of school administration if it is misused or abused.

Network

School Local Network

The district provides a local network to share printers, documents, and other data. Each student is assigned an account on the network and a private network drive to use for storing their class work. The private network drive is the property of USD 369, is intended only for school-related files, and must not contain executables (such as programs and applications), runnable scripts (that are not school related), copyrighted material that the student doesn't own the copyright to, or any other non-school related or inappropriate data.

It is the responsibility of each student to keep his or her password secret at all times. Any inappropriate activity performed under a student's account will be the responsibility of that student. If a student suspects another person knows his or her password, that student needs to report it to school staff. Students must have permission to use school computers and should only be logged in under their own name.

Ad-hoc Networks

Ad-hoc networks are small networks created, either wirelessly or wired, using a variety of technologies. Bluetooth, wifi 802.11a/b/g/n/ac and infrared are several wireless technologies that allow the creation of small, autonomous networks that are outside of the district network. Students must not create nor use ad-hoc networks without permission from the Technology Coordinator or other technology staff members.

Internet

Internet Use

All computers in the school district have the ability to connect to and use the Internet connection. The Internet may be used for research and educational projects. It is not provided for entertainment purposes. Access to the Internet is a privilege that may be revoked at any time. Only school-owned computer hardware may be allowed to access the Internet.

Accessing, downloading, printing and/or sharing obscene, pornographic, illegal, gang related*, drug related* or gambling content is strictly forbidden. Illegal content and illegal activity carried out on the network or Internet connection may result in law enforcement being notified.
*Only school-related research is acceptable and prior permission must be obtained to do such research.

Privacy on the Internet

Students must not give out personal information like their address, full name, phone numbers, social security number,

driver's license or credit card information to anyone at any time on the Internet. That information should remain private at all times. There is no such thing as anonymity when on the Internet as all communications can be tracked by anyone between the computer and the web site. The Child Internet Protection Act prohibits the use of unfiltered communications on the Internet. Social networks, forums, chat and instant message sites and applications are not to be used on campus. We track Internet activity for all computers on our network for safety and security reasons.

Email

The school district provides access to filtered and monitored email for district communications. With this email system, students may only communicate with students and faculty within the school district. Students may access email accounts away from the school, but email messages are still monitored and restricted just as if they are at school. Students in grades 6-12 may have email accounts created for the purpose of educational collaboration with other schools. The email is provided for educational use only, and it is a privilege to use this service. If the parents do not want their student(s) to have access to district email, please, call the office and arrangements will be made.

Communications should be polite and not abusive (do not be a bully). Use appropriate language when writing messages (do not use obscene or vulgar language). Do not send messages that contain obscene content in any format (text, images, videos, etc). There is absolutely no guarantee that a message is neither private nor anonymous. Messages sent over the Internet may be intercepted and read.

It is strictly forbidden for students to use or attempt to use any other email service other than the district provided email while on campus.

Peer-to-Peer File Sharing

There are several Internet-based services that allow file sharing directly from one computer to another called peer-to-peer file sharing. Students may not access any peer-to-peer sites or software.

Content Filter

The entire district is protected by a content filter to help protect students from inappropriate sites. Even with the content filter in place, it is still possible to access some inappropriate sites that are not known to us. No content filter is perfect. If a student discovers an inappropriate site, they are to go back in their browser and inform their teacher immediately.

There are numerous websites and applications that provide ways to circumvent (or bypass) content filters and more are added each day. Students are not allowed to use any of these sites. If a student reaches a blocked site, the student needs to notify the teacher immediately.

General Computer Use

Copyright

In the United States, when a work (textual and all art forms) is created, a photo or video is recorded or audio is recorded, that work is automatically copyrighted. Almost all content on the Internet is copyrighted, either automatically or formally. All students must obey copyright laws and only use work they have permission to use. Please, refer to the United States copyright law for specific questions (you may get more information at this site: http://www.copyright.gov). Like all other illegal activity, law enforcement may be notified if copyright laws are not obeyed.

Cracking (or hacking)

Cracking is the act of breaking into a computer or network and gaining elevated access that was not explicitly given. It is strictly forbidden to attempt to break into any district-owned hardware (including workstations and servers), network accounts, email accounts and any websites or servers on the Internet from the district-provided network or Internet connection. Any attempts to circumvent any security on the network or Internet connection is a form of cracking or hacking and may be turned over to law enforcement. There will be no tolerance for this activity.

Removable Media

The only removable media allowed to be attached to a school computer is a USB flash drive. No MP3 players, USB hard drives, smartphones or any other device other than a USB flash drive may be attached to a school computer under any circumstance. No executables (such as applications or programs) may be run off a USB flash drive. The USB flash drive may only be used to access documents and is subject to searches.

Non-school Computers

Students in grades PK-5 are not permitted to bring electronic devices from home. Students in grades 6-12 are allowed to bring devices from home for school use (with permission). These terms are covered under the district's *"Bring Your Own Device" Terms and Conditions*.

Vandalism

Vandalism, destruction, or unauthorized modifications to or attempts to modify any district computer or network hardware, computer peripherals, software and data are strictly prohibited. Students are financially responsible for damages resulting from vandalism, destruction, or unauthorized modifications to any district property. A student needs to report anything not working to their teacher. If the student discovers any vandalism, he or she should also report this as soon as possible.

Burrton USD 369:

- **reserves the right to log and view Internet use and to monitor file server space utilization by users.**

- **reserves the right to remove a user from the network to prevent further unauthorized activity.**

- **provides Internet filtering.**

- **does not allow unauthorized disclosure, use, and dissemination of personal information regarding minors.**

Accepting this Policy

Students must accept this policy to use any computers, network, Internet access and email.

Student Acceptable Use Policy Agreement
For Network Access and Internet Safety

I understand and will abide by USD 369 Burrton School District's terms and conditions for the use of the district computing hardware, network and Internet access. I further understand any violation of these conditions may result in disciplinary action where appropriate.

☐ I agree to the above statement.   ☐ I choose to opt out of having Internet/network access

User's Full Name:_____ Grade:_____

User's Signature:_____ Date: _____

Parent/Guardian Signature:_____ Date: _____
: