**Beecher City Unit District #20**

*Technology Acceptable Use Policy*

 **Technology Mission Statement**

The technology mission of Beecher City Community Unit School District #20 is to provide current technology to educate and encourage students, teachers, and community to develop practical technological skills that will prepare them for change in the 21st century

 **Electronic Network Access**

All use of the Internet and Network Access shall be consistent with the District’s goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. Authorization does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any** **user to follow the terms of the *Authorization for Electronic Network Access* will** **result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

**Terms and Conditions**

1. **Acceptable Use** – Access to the District’s electronic networks must be (a) for the purpose of education or research, and be consistent with the educational objectives of the District, or (b) for a legitimate business use.
2. **Privileges –** The use of the District’s electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator will make all decisions regarding whether or not a user has violated *Authorization* and may deny, revoke, or suspend access at any time; his or her decision is final.
3. **Unacceptable Use** – The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:
	1. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State law
	2. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused
	3. Downloading copyrighted material for other than personal use
	4. Using the network for private financial or commercial gain
	5. Wastefully using resources, such as file space
	6. Hacking or gaining unauthorized access to files, resources, or entities
	7. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature
	8. Using another user’s account or password
	9. Posting material authored or created by another without his/her consent.
	10. Posting anonymous messages
	11. Using the network for commercial or private advertising
	12. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material
	13. Using the network while access privileges are suspended or revoked.
4. **Network Etiquette** – You are expected to abide by the generally accepted rules of network etiquette. These include but are not limited to, the following:
	1. Be polite. Do not become abusive in your messages to others.
	2. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
	3. Do not reveal the personal information, including the addresses or telephone numbers of students or colleagues.
	4. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
	5. Do not use the network in any way that would disrupt its use by other users.
	6. Consider all communications and information accessible via the network to be private property.
5. **No Warranties** – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, nondeliveries, missed-deliveries, or service interruptions caused by its negligence or the user’s errors or omissions. Use of any information obtained via the Internet is at the users own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
6. **Indemnification** – The user agrees to indemnify the School District for any losses costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this *Authorization.*
7. **Security –** Network security is a high priority. If you can identify a security problem on the Internet, you must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Attempts to log-on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.
8. **Vandalism–** Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.
9. **Telephone Charges –** The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.
10. **Copyright Web Publishing Rights** – Copyright law and District policy prohibit the re-publishing of text or graphics found on the Web or on District Web sites or file servers, without explicit written permission.
	1. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
	2. Students and staff engaged in producing Web pages must provide e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of “public domain” documents must be provided.
	3. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.
	4. The “fair use” rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
	5. Student work may only be published if there is written permission from both the parent/guardian and student.
11. **Use of Electronic Mail**
	1. The district reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account’s user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
	2. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be translated in an e-mail message that would be inappropriate in a letter or memorandum.
	3. Electronic messages transmitted via the School District’s Internet gateway carry with them an identification of the user’s Internet “domain”. This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this School District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
	4. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message’s authenticity and the nature of the file so transmitted.

**Internet Safety**

1. Internet access is limited to only those “acceptable uses” as detailed in these procedures. Internet safety is almost assured if users will not engage in “unacceptable uses” as detailed in this Authorization, and otherwise follow this Authorization.
2. Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in this Authorization.
3. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children’s Internet Protection Act and as determined by the Superintendent or designee.
4. The system administrator and Building Principals shall monitor student Internet access.

**Mobile Electronic Devices**

**Definition**: Mobile electronic devices for the purposes of this policy will only include laptops, Tablets, e-readers, and personal iPads.

1. Use of mobile electronic devices must be for the purpose of education or research, and be consistent with the educational objectives of the District.
2. Use of mobile electronic devices by students must be approved by the building level administration and the classroom instructor or supervisor.
3. A student will not be allowed to use a mobile electronic device in a way that is in violation of the student handbook p. 28.
4. When using mobile electronic devices at school the only Wi-Fi connection the student is allowed to use is the Wi-Fi connection provided by the Unit #20 School District. All use of other wireless connections is prohibited.
5. Use of mobile electronic devices is limited to scheduled instructional class time and scheduled study time. Mobile electronic devices can only be used in academic classroom areas, and the designated “study hall” area. Mobile electronic devices can only be used at the above times and locations with the approval and supervision of a Unit 20 staff member.
6. Any use of mobile electronic devices is strictly prohibited in non-academic areas including but not limited to locker rooms and restrooms, whether here or at another facility where a school activity is occurring.
7. The recording capabilities of a mobile electronic device can only be used with the permission of the building administration and the classroom instructor or supervisor. The recording capabilities of the mobile electronic device can only be used for purposes of education, and must be consistent with the instructional objectives of the Beecher City Unit #20 School District. Students who use the recording capabilities of a mobile electronic device inappropriately will face discipline consequences that could include detentions, suspensions, and recommendation for expulsion from school.
8. Students who choose to bring their personal mobile electronic device to school will understand that school personnel will not be responsible for troubleshooting or supporting the use of that device.
9. Mobile electronic devices are popular theft items. The District is not responsible for the loss, theft, damage, or vandalism to student mobile electronic devices. Students and parents are strongly encouraged to ensure that if students have mobile electronic devices in their possession they should not leave them unattended or unsecured. The school district is not required to provide storage for mobile electronic devices.

**Discipline for Misuse of Mobile Electronic Device:** Misuse of a mobile electronic device will result in disciplinary action including but not limited to the device being confiscated, the student not being allowed to bring a Mobile Electronic Device to school, the student losing all network and computer access privileges while at school, the student being removed from the class, and if necessary other appropriate discipline or legal action that would apply. \*\* Beecher City Unit #20 reserves the right to make changes to the policy

**AUTHORIZATION FOR USE OF STUDENT PICTURES/STUDENT WORK**

Student pictures will be posted on the website only if there is a signed parent permission form with the school.

**ELECTRONIC NETWORK ACCESS AUTHORIZATION**

Students and parents must sign the *Authorization for Electronic Network Access* form in order to have electronic network privileges.

**IMPORTANT TECHNOLOGY REMINDERS**

***E-Mail***

Students ***will not***be allowed personal E-mail privileges at Beecher Junior Senior High School. Only E-Mail essential to class assignments approved by the school will be permitted.

***Chat Rooms***

Access of chat rooms is prohibited.

***Inappropriate sites***

Steps have been implemented to protect students from inappropriate Internet sites that promote pornography, hate, and violence. If a student accidentally accesses such a site they are to report it immediately to their supervisor or risk disciplinary action.

***Penalties for inappropriate use***

Chat Room/Chatting 1st offense Detention and 6 week suspension of access
 2nd offense Detention and 12 week suspension of access

 3rd offense Detention and 1 year suspension of access

Unauthorized E-mail 1st offense Detention and 6 week suspension of access
 2nd offense Detention and 12 week suspension of access

 3rd offense Detention and 1 year suspension of access

Inappropriate Sites 1st offense Detention and 6 week suspension of access
 2nd offense Detention and 12 week suspension of access

 3rd offense Detention and 1 year suspension of access

Using Another Students Password 1st offense Detention and 6 week suspension of access
 2nd offense Detention and 12 week suspension of access

 3rd offense Detention and 1 year suspension of access

Pornography 1st offense In School Suspension and 18 week suspension of access
 2nd offense Out of School Suspension and 1 year suspension of access

Using Teacher’s Password 1st offense In School Suspension and 1 year suspension of access.

**\*\*Punishment for violations not specifically covered will be determined by the administration.**