POLICY 4177

Responsible Computer Use

A. It is the policy of Box Elder School District to permit students, patrons, and employees to have computer and Internet access under approved regulations and guidelines, to include those listed in the Children's Internet Protection Act, Federal & State Law, and policies adopted by the Board of education. It is expected that students, patrons, and employees accessing district network resources will adhere to high standards of digital citizenship and conduct themselves in a responsible, decent, ethical, and polite manner.

1. Access to the district network is permitted primarily for instructional purposes and is a privilege not a right. Limited personal use of the district network is permitted if the uses pose no tangible cost to the District, does not unduly burden or cause damage to the district's computer or network resources, and does not adversely affect a student's academic performance or an employee's job performance.

2. All devices accessing the district network will have content filtered in accordance with federal and state law, including the Children's Internet Protection Act and the Family Education Rights and Privacy Act.

3. Privately owned devices accessing the district network may be required to allow device management as specified by the district technology department.

4. Students, patrons, and employees must agree to the terms and conditions of the associated acceptable use agreement prior being granted access to district computers and network resources.

B. Prohibited Uses: The following uses of the District's computers and network resources are prohibited.

1. Using an account other than one's own and any attempt to gain unauthorized access to accounts on the network.

2. Manipulating or attempting to manipulate, reconfigure or damage district hardware, software or network settings.

3. The use of games, chat rooms, blog, social networking sites, and instant messaging that is not directly related to curriculum development, instruction, work assignment, or assigned learning experience.

4. Degrading or attempting to degrade or disrupt networking equipment or services.

5. Using computers or network resources for any illegal activity. This includes, but is not limited to transmitting or receiving:

a. threatening or obscene material,

b. material protected by trade secrets or copyrighted without proper permission,

c. the design or detailed information pertaining to explosive devices,

d. criminal or terrorist acts,

e. sexism or sexual harassment,

f. pornography,

g. gambling,

h. illegal solicitation,

i. racism, or

j. inappropriate language.

6. Transmitting or receiving any material reflecting adversely upon individuals because of their race, national origin, sexual orientation, gender, religion, or disability.

7. Using the district computers or network resources for personal financial gain, personal business and product advertisement, or personal use for religious or political lobbying (including student body elections or representation elections for employees).

8. Destroying or attempting to destroy or degrade data of another user, another agency or network. This includes uploading or downloading, or the creation of digital viruses or malware.

9. Violating the privacy of another by disclosing confidential information about other individuals, if the disclosure is not allowed by federal or state law or district policy.

10. Posting personal communications without the original author's consent or posting anonymous messages.

11. Bypassing or attempting to bypass filters and security via proxy servers, VPN access, connecting personal wireless access points, or other means.

12. Any content that disrupts the educational environment.

13. Erasing, expiring, or resetting memory cache, webpage links, or HTTP location history without permission.

14. Downloading, uploading, installing or executing applications, unauthorized programs or software.

C. Discipline: Irresponsible/inappropriate use of digital devices or network resources may result in the loss of network privileges, disciplinary action, termination of employment, and/or referral to legal authorities and the Utah Professional Practices Commission.

1. The technology department monitors network activity and will communicate any violations or suspected violations of this policy or the responsible use agreements to the appropriate administrator. There is no expectation of privacy on the district network.

2. If employees, students, or patrons become aware of any violations of this policy or the responsible use agreements they should report the violation or suspected violation to their teacher or building/District administrator.

3. Students, patrons, employees are liable for replacement costs of any computer/network resources damaged by neglect or willful disregard.

D. Security:

1. Any passwords issued to users must not be shared with or disclosed to other users without specific authorization from the administrator.

2. Passwords should be changed regularly in accordance with industry standards.

3. Users should not leave workstations without logging out or locking the device.

E. Privately owned devices: Students, patrons, and employees have the privilege of using privately owned digital devices on the District network in compliance with this policy and school/classroom rules.

1. Teachers, building administrators and district staff may confiscate and search a privately owned device if federal or state law, district policy, or school or class rules are violated.

2. Devices confiscated under the provisions of this policy may be turned over to law enforcement agencies for further investigation.

F. Disclaimer: The District makes no guarantee of the completeness or accuracy of any information provided on the network. It makes no promise or warranty to maintain or update its network or the information contained or made available to the public, its employees, and students. The District may suspend or discontinue these services at any time.

1. The District specifically disavows legal responsibility for what a user may find on another external site or for personal opinions of individuals posted on any site.

2. A user assumes the risk of use or reliance on any information obtained through the network.

3. The District will not be responsible for any damages a user suffers while on the system, including loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by negligence, errors, or omissions.