Responsible Computer/Digital Resource Agreement - Employee

Violations of the Responsible Computer/Digital Resources Policy may cause an employee's access privileges to be revoked, and/or personal disciplinary action up to and including termination of employment. 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 an employee's job performance.

A. Employee will:
    1. Keep usernames and passwords private. Usernames and passwords may not be shared with anyone (including other staff, volunteers, students, student aides) nor should you use another individual's usernames and passwords.
        a. Student teachers are required to share their BESD username and password information with their mentor teacher.
        b. If, for any reason, it becomes necessary for another person (i.e., long term sub, student teacher, etc.) to have access to an employee's educational account/s computer or network resources, the principal should contact the school district IT department.
    2. Maintain copies (back-up) of work-related data.
    3. Treat student usernames and passwords and other protected data with confidentiality.
    4. Ensure all personal forms of digital storage accessed on the network is free from viruses/malware and is in compliance with all federal and state law and is not disruptive to the educational environment.
    5. Ensure that all student data is compiled, stored, and distributed in accordance with the Family Educational Rights and Privacy Act (FERPA), state data privacy laws, and Policy 5140 Education and Family Privacy Rights.
    6. Use email accounts provided to employees for professional purposes only. The email account provided should be used for all school district business. (Outside email accounts (i.e., Hotmail, Gmail, Yahoo, etc.) are not supported with technical assistance from the school district and if used for work related communication may become subject to GRAMA requests.
    7. Enforce the Responsible Computer/Digital Resources Use Policy while supervising students. Notify administration and the district IT security team of any violations of Policy 4177 Responsible Computer Use and 4178 Internet Policy.
    8. Abide by the Box Elder School District Policy 3084 Educational Appropriate Postings when posting any materials to the web.

9. Directly supervise students' use of the network and/or internet. Train students to immediately terminate viewing content and notify a school official if inappropriate content is discovered on district digital technology (i.e., computers, internet, etc.).
10. Will not use their District email for a political purpose advocate for or against.

B. Employee will not:
   1. Use the internet for illegal or inappropriate purposes to access materials that are objectionable in a public-school environment, or in support of such activities. Additionally, use language that is deemed to be vulgar or using the Internet to defame or demean any person.
   2. Connect or install any computer hardware, components, or software, which are not school system property, without prior approval of the district technology department. Connect or install privately owned networking hardware or software, components, or routers to the District corporate networks without authorization from the technology department.
   3. Install or download, on district devices, any software without the approval of the Technology Department.
   4. Circumvent or attempt to circumvent the district's content filtering system(s).
   5. Use the district network for personal financial gain or advertising.
   6. Engage students (individual or group) on social networking sites, by private text message, or in any other digital format whether in class or outside of school for any non-professional educational reason. Electronic communication with students should be limited to providing general information related to coursework, and/or school activities.
   7. Transmit any material in violation of any U.S., Utah State or District policy regulation or statute is prohibited. This includes, but is not limited to: copyrighted material; threatening or obscene materials, anarchist or terrorist information, or material protected by trade secrets.

C. Employee Understands:
   1. Users have no expectation of privacy regarding their use of District property, network and/or internet access or files, including email. All information is subject to GRAMA laws, acknowledge that all electronic messages and files stored on school-based computers or traversed across the District's networks <u>are considered public records</u> and may be reviewed by administrators and/or designees to maintain system integrity and insure that users are acting responsibly.
   2. In accordance with the Government Records Access Management Act (GRAMA), Child's Internet Protection Act (CIPA), and/or Family Educational Rights and Privacy Act (FERPA), I will not publish personally identifiable information such as student's full name, photograph, etc. over the internet without specific documented consent from the parent or legal guardian.

3. All devices accessing the District network on or off school district property will have content filtered in accordance with federal and state law, including compliance with the Children's Internet Protection Act (CIPA) and the Family Education Rights and Privacy Act (FERPA).
4. District provided and privately owned devices accessing the District network or its resources may be required to allow device management as specified by the District Technology Department.

D. User Signature of Agreement:

I understand any violations of the above provisions may result in the loss of employment. I agree to report any misuse of the electronic information resources to my building administrator. Misuse comes in many forms, but can be viewed as any messages, information or graphics sent or received (unsolicited, inappropriate messages should be reported to the building administrator) that include or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other listings as described above. Rules of conduct are described in this Employee Responsible Computer/Digital Resources Agreement.

I have read this agreement and understand that Internet sites are filtered and that my district computer Internet use is being monitored. I hereby agree to comply with the above-described conditions of acceptable use.

User Name (Please Print) _____

User Signature_____ Date_____