Title: Appropriate Use of Computers, Computer Network and the Internet –Employees

Computing devices, data networks, and Internet access that are provided by the school district are the property of the school district and shall be used only for lawful purposes. Such systems may not be confidential, and employees should have no expectation of privacy in any materials therein. Computing devices include but are not limited to computers, laptops, cloud computing, telephones, smart phones, tablets, printers, faxes, and multi-function devices.

The following are the established expectations and standards of the Council Bluffs Community School District regarding the acceptable use by employees of computing devices, data networks, Internet access and other online services provided by the District. Employees include those contracted, service partners or others representing the District. This policy applies to any computer, network or Internet/online material, including material that the employee believes to be private**.**

The District requires employees to learn to use computing devices, data networks, enterprise software systems, electronic mail, the Internet, and telecommunications tools and apply them in the appropriate ways to the performance of tasks associated with their positions and assignments.

Employees shall communicate in a professional manner consistent with the applicable laws and District policies, including those governing the behavior of school employee's copyrights and confidentiality of employee and student records and other information. All applicable laws & policies apply when using technology.

Employees are encouraged to use the district-approved and monitored platforms of Google Workspace apps including but not limited to Gmail, Meet, Google Voice, or Google Chat and Google Classroom.

All other contact, including but not limited to phone calls from employee personal landline or personal mobile/cell phones, text messaging (SMS), private messaging and in-app messaging, should only be used if the other platforms are not available or sufficient:

All communication between staff and students shall:

- Be factual and professional in manner and message
- Take into consideration the time of day and day of week**,** including limiting communication to school day hours when possible
- Adhere to all District policies, including those outlined above.

Title: Appropriate Use of Computers, Computer Network and the Internet –Employees

Use of District, computing devices, data networks, and the Internet, and any communications thereby should not be considered by employees to be private. The District's Chief Technology Officer, other administrators or designated staff may from time to time, and without prior notice, examine all computing devices and Internet activities and review directories, messages, email and files to ascertain compliance with guidelines for acceptable use. Any disclosure of the contents are subject to the discretion of the District administration and/or when required by law, by policies of the District, or to investigate complaints regarding electronic mail or files which are alleged to contain inappropriate material or to have been in violation of District policy. The Chief Technology Officer, other administrators or designated staff have the authority to copy, disclose, move, alter or delete files as may be necessary in the sole judgment of the Chief Technology Officer, other administrators or designated staff.

Individual staff members should not allow anyone else to access or use the District's computing devices or data network or the Internet by using the employee's personal identification number or password. Employees are responsible for the security of their own electronic passwords that allow access to district resources**.** Employees will be held responsible for any misuse of their computing device, electronic communication, or data network access by themselves or by others when the employee has failed to follow appropriate security measures.

Employees authorized to allow student access to the District's data network and Internet may do so only according to the student access policy and are responsible for supervising student access. Employees who allow student access to computer networks and the Internet in violation of the student access policy may be subject to disciplinary action up to and including termination.

The following uses of District computing devices, data networks, and Internet access are expressly prohibited on the part of District employees:

- Creating, accessing, uploading, downloading, transmitting or distributing pornographic, obscene, profane, abusive, threatening, sexually explicit or otherwise inappropriate material, or material encouraging or promoting discrimination towards individuals or groups of individuals based upon a legally protected trait or characteristic.
- Uses which violate any local, state or federal statute or regulation.

Title: Appropriate Use of Computers, Computer Network and the Internet –Employees

- Accessing another individual's materials, information, or files without authorization (authority)
- Uses which violate copyright laws or otherwise misuse the intellectual property of another individual or organization.
- Unauthorized use of another's password.
- Any unauthorized access or malicious attempts to damage hardware/software or networks or to destroy the data of another user, including creating, loading or intentionally introducing viruses.
- Using computing devices, data network or Internet for commercial purposes or personal purposes which interfere with job performance or function of the workplace, or other purposes not consistent with the educational objectives of the District.
- Harassing, insulting, or threatening harm or embarrassment of others.
- Gaining unauthorized access to others' resources or entities.
- Invading the privacy of individuals without authorization.
- Altering the operation of computing devices as set by the Chief Technology Officer.
- Failing to follow the law or District policy while using computing devices or data networks or accessing the Internet or failing to follow any other policies or guidelines established by District administration or the employee's supervisor and failure to follow instructions of supervisors.
- Using the system to communicate, publish or display defamatory materials, rumors, disparaging portrayals or any other information which is known to be false or misleading.

Employees are responsible for maintaining a safe and secure school environment. This includes computing devices and the data network. Employees shall change passwords when directed by the Chief Technology Officer or designee. Employees determined to be a security risk may be restricted to monitored access.

The District makes no warranties of any kind, whether expressed or implied, for the access it is providing. The District is not responsible for any damages suffered by employees or by third persons. This includes loss of data resulting from delays, non-deliveries, delivery failures, or service interruptions caused by the District or employee errors or omissions. Use of any information obtained via the Internet is at the user's risk. The District is not responsible for the accuracy or quality of information accessed through its system.

Title: Appropriate Use of Computers, Computer Network and the Internet –Employees

The District will use technology protection measures to guard against employee access of inappropriate Internet sites**,** as required by applicable law.

Employees who violate any part of this policy will be subject to disciplinary action, which can include employment consequences up to and including termination.

Cross References:

402, 405, 425.1, 512, 617, 617.1

Legal References:

Iowa Code § 279.8, 47 U.S.C. § 254

Approved: Jul. 21, 1998

Reviewed: _____

Revised: April 28, 2003
March 25, 2008
March 30, 2010
March 22, 2011
March 22, 2016
June 25, 2019
April 14, 2020
May 23, 2023