STAFF ACCEPTABLE USE OF TECHNOLOGY

This policy applies to all District workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to district technology resources.

Responsibilities: The School District Technology Director will be responsible for ensuring the implementation of the requirements of this policy.

Compliance: Failure to comply with this or any other security policy may result in disciplinary actions up to and including termination of employment. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal laws and rules to include the Family Educational Rights and Privacy Act (FERPA).

1.0 PURPOSE

1.1 Use of computers and network resources by employees of the District and other permitted users (referred to herein collectively as "Staff") is permitted and encouraged where such use supports the goals and objectives of the District. Communications and computer technology at the District are provided and maintained for educational and administrative purposes.

1.2 Personal use of communications and computer technology at the District is prohibited during the Staff member's student contact hours. During all other times, limited personal use is allowable when it is brief in nature, does not interfere or conflict with the Staff member's responsibilities and conforms to other District policies, including content, computer use and student data security policies. Notwithstanding the foregoing, school district emails and accounts are strictly limited to school use only. School district emails and accounts should not be used for personal use (e.g. banking, shopping, communications).

1.3 Use of personal (non-District owned) computers, devices and technology (including cell phones) for District purposes is discouraged. Employees are encouraged to use School District computers, devices and technology for School District purposes. Certain staff may be allowed to use personal cell phones for school district purposes as determined by the Superintendent and/or his/her designee. Employees who use their personal devices or technology for school district communications shall disclose such communications (and only such communications) to the school district upon request of the building principal or Superintendent.

2.0 ACCESS TO TECHNOLOGY EQUIPMENT AND SERVICES

2.1 Access to technology is provided to facilitate the instructional and administrative tasks performed by District Staff. The technology provided will align with the requirements of each Staff member's job functions.

2.2 Computer files and interactions over digital networks, including email, chat, voicemail, video, and web search, are not exclusively private. It should be understood that the District Technology Department will have access to computer files and communications. When the administration believes a staff member may have engaged in misconduct or when possible misconduct is identified as a result of general administration and support of the District technology systems, the Superintendent and/or designee may review computer usage and/or information accessed or stored by school district employees.

2.3 To ensure proper function, District administrators and their designees may monitor the District’s technology resources, including email, chat, voicemail, video, and Internet usage, at any time without advance notice or consent.

2.4 School District employees have no expectation of privacy in communications they send or receive on the District’s computers or network system, or as to sites and information accessed utilizing District computers or the networking system. The District has the right to monitor or review any communications sent or received, as well as information regarding sites and/or information accessed.

3.0 ACCEPTABLE USE

3.1 It is a general policy that technology resources are to be used in a responsible, efficient, ethical, and legal manner in support of District operational and educational programs. The use of technology resources is a privilege, not a right.

3.2 Site administrators, directors or supervisors may set more restrictive guidelines for Staff members in their areas of responsibility.

3.3 The School District shall use internet filters to restrict access to inappropriate, illegal or potentially offensive materials. Disciplinary action shall be taken against any person who tampers with the filters. Staff members shall report any instances where the Acceptable Use Policy, network security, or data security may be violated. Staff members shall also report inappropriate Internet websites to the Technology Department.

4.0 PROPER USE AND CARE

4.1 Before operating any equipment, users will be made familiar with the basics of safety and damage prevention, and trained on proper care and operation.

4.2 Staff are responsible for damage to or loss of district technology resources due to misuse or negligence. Users are liable for intentionally inflicted damage.

4.3 Staff should not attempt repairs without authorization or support from designated District or school site personnel. Volunteers, parents, family members, or friends of Staff members or students are not authorized to attempt repairs on District equipment.

4.4 Staff shall not install or modify applications without approval and support of the District Technology Department or designated technology teachers and support staff at school sites. Staff shall not download or install copyrighted software without proper licensing. Copyrighted material shall be posted online only in accordance with applicable copyright laws.

4.5 Staff should not connect personally owned technology equipment to the District network without approval by the Technology Director.

5.0 PERSONAL RESPONSIBILITY

5.1 All District technology equipment is District property.

5.2 Staff members shall not search, view or otherwise access, post, submit, publish, store, or display harmful or inappropriate material that is threatening, obscene, disruptive, pornographic or sexually explicit, or that could be construed as harassment or disparagement of others.

5.3 Staff members shall not use the system to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.

5.4 Staff members shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee. In addition, District technology resources may not be used to conduct political or religious activities. District email may not be used to advertise or solicit for non-District sponsored events, activities or organizations.

5.5 The District maintains a public Internet site. Any information to be posted on the public website must be approved through administrators (or their designee). Principals or his/her designees must approve all postings on school Web pages. Restrictions apply to links to other sites that may not be appropriate and to personal information or pictures of students without parental consent.

5.6 Staff members shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, modify, or forge other users' mail or other online communications.

5.7 Staff members shall not develop any classroom or work-related websites, blogs, forums, or similar online communications representing the District or using district equipment or resources without prior approval. Such sites shall be subject to rules and guidelines established for District online publishing activities including, but not limited to, copyright laws, privacy rights, student data protections, and prohibitions against obscene, libelous, and slanderous content. Because of the unfiltered nature of blogs any such site shall include a disclaimer that the District is not responsible for the content of the messages. The District retains the right to delete material on any such online communications.

5.8 Users shall report any security problems or misuse of the services to the Superintendent or designee.

5.9 The Technology Director and Department will take an active role in backing up server data. However, statistics show that backups may not restore correctly. Therefore, ultimately each staff member is responsible for backing up their own data in at least two different locations to ensure that their data is not lost (i.e. on a cloud server such as Google Drive, and/or external storage device, etc.).Employees shall not communicate, disseminate, distribute or share confidential information to unauthorized parties. Nothing in this policy shall be construed as allowing any employee to communicate, disseminate, distribute or share confidential information with unauthorized persons.

6.0 SECURITY AND PASSWORDS

6.1 To maintain security, users are issued unique User ID's and passwords to enable network access. Do not share passwords. If the password has or may have been compromised, contact the Technology Department for assistance.

7.0 PENALTIES FOR VIOLATIONS

7.1 Violation of the Acceptable Use Policy may result in a reduction or loss of access privileges. In many cases, access privileges may be essential to job functions. Additionally, those failing to follow the guidelines contained in this policy will be subject to disciplinary action up to and including termination of employment.

8.0 EMPLOYEE ACKNOWLEDGEMENT

8.1 All Staff members of the District who have access to district technology will be required to acknowledge upon hire that they have received, read and accepted this Administrative Regulation.

Annually this Administrative Regulation will be sent to all employees.

W.S. 21-2-202 (a)(xxxvii)(A)-(E)

First Reading: 5-1-23
Second Reading: 6-12-23