EMPLOYEE USE OF COMPUTERS, THE INTERNET AND ELECTRONIC COMMUNICATIONS

1.0 The District supports the use of the Internet and electronic communications by all employees to improve teaching and learning through interpersonal communication, access to information, research, training and collaboration and dissemination of successful educational practices, methods and materials.

2.0 The Internet is a fluid environment in which information is constantly changing. The District will make every reasonable effort to ensure that this educational resource is used appropriately and responsibly. Administrators, teachers, and staff have a professional responsibility to work together to help students develop the intellectual skills needed to evaluate and choose information sources, to identify information appropriate to their age and developmental levels, create effective and appropriate information, and to evaluate and use information to meet their educational goals.

3.0 Employees shall take responsibility for their own use of District computers and computer systems. Employees shall use District computers and computer systems in a responsible, efficient, ethical and legal manner. Employees are responsible for exercising good judgment when utilizing District resources and should be wary of unknown email solicitations, pop-up boxes or writing anything in an email message that is inappropriate to say to others face-to-face.

4.0 **Employee Use is a Privilege**. Use of District computers, the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Employee use of District computers, the Internet and electronic communications is a privilege, not a right. Violations of this policy may result in the loss of the privilege to use these tools, as well as disciplinary action up to and including dismissal and/or legal action. The District may deny, revoke or suspend access to District technology or close accounts at any time and without notice.

5.0 **No Expectation of Privacy**. District computers and computer systems are owned by the District and are intended for educational purposes and District business at all times. Employees shall have no expectation of privacy when using District computers, the Internet or electronic communications. The District reserves the right to monitor, inspect, copy, review and store, at any time and without prior notice, all usage of District computers and computer systems, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through District computers and computer systems shall remain the property of the District. Electronic messages sent or received by the Board, the District's employees or students, including electronic mail on District-owned equipment, as well as other documents generated through use of the District's system may be considered a public record subject to disclosure or inspection under the Colorado Open Records Act.

6.0 **Accounts and Passwords**. Employees are expected to protect personal login and password information, and should not share access with anyone, including a co-worker, student, parents/guardian or volunteer. When necessary to conduct the business affairs of the District, the Superintendent or designee may grant permission to share access. Employees may be directed to disclose login and password information by a supervisor.

7.0 **Prohibited Uses**. Because technology and methods of using technology are constantly evolving, every unacceptable use of District computers and computer systems cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following.

7.1 No employee shall access, create, transmit, retransmit or forward material or information that:

7.1.1 Promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons.

7.1.2 Contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, or material that is harmful to minors.

7.1.3 Harasses, bullies, intimidates, threatens, demeans, or promotes violence or hatred against another person or group of persons with regard to race, color, sex, age, religion, creed, national origin, ancestry, genetic information, marital status, sexual orientation, gender identity, disability, or conditions related to childbirth.

7.1.4 Plagiarizes the work of another.

7.1.5 Uses inappropriate or profane language or depictions.

7.1.6 Is knowingly false.

7.1.7 Violates any federal or state law, including but not limited to copyright or material that contains personal information, including information protected by confidentiality laws.

7.1.8 Impersonates another person.

7.1.9 Is intended to solicit, proselytize, advocate, or communicate the views of a non-school sponsored organization.

7.2 The following activities are also prohibited:

7.2.1 Using information systems or resources for personal gain or outside the scope of employment.

7.2.2 Attempting to gain unauthorized access to any other computer, network or security account including attempts to log in as a system administrator.

7.2.3 Any malicious attempt to harm or destroy District data, data of another user, or other District computing facilities.

7.2.4 Using or attempting to use proxy servers, or otherwise evade, disable, or "crack" passwords or other security provisions of the systems on the network or intercepting or altering network packets.

7.2.5 Downloading, installing, storing or using malicious software, viruses, "cracking," and keystroke monitoring software.

7.2.6 Intentionally interfering with or disrupting another information technology user's work as well as the proper function of information processing and network services or equipment.

7.2.7 Leaving an active system unattended, thereby allowing an unauthorized person to gain access to District resources through the user's login session.

7.2.8 Using a computer for unlawful purposes.

7.2.9 Altering technology equipment (hardware or software) without permission from the I.T. department.

7.2.10 Taking home technology equipment (hardware or software) without permission of the employee's supervisor or designee.

8.0 **Electronic Communications**. The District may provide electronic communication services for employees. The District reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all electronic communication content composed, sent over, by, or through District computers or computer systems or with a District-provided account, even if composed and sent during non-work/school hours or from a non-District site, and to disclose the information to law enforcement or other third parties, as appropriate.

8.1 Employees shall use District-provided electronic communications accounts and not personal accounts when acting in the course and scope of employment and conducting business on behalf of the District.

8.2 Employees are permitted to affix a signature block to email messages that contains name, job title and departmental information and contact information. The District approved notices that may be included at the end of the signature block of email messages in are attached hereto in Exhibit A. Aside from the information described above, employees shall not affix quotations, slogans, facts, mission statements, taglines or other information as part of the signature block.

9.0 **Security**. Security and integrity of District computer systems and information is a high priority and requires participation of all employees. Employees who identify a security problem while using the Internet or electronic communications should immediately notify the IT Help Desk and avoid demonstrating the problem to other users. Student or employee information stored in electronic format shall not be taken home on a laptop or transferred to an external device for home or outside use unless District data security and encryption procedures are followed.

9.1 To protect hardware, software, and information, employees must follow security procedures and standards created by the District's Information Technology Department when working at home or an alternative workplace.

10.0 **Confidentiality**. Employees shall only access, receive, transmit or retransmit material regarding students, parents or District employees that is protected by confidentiality laws in accordance with law and District Policy. Employees shall handle all employee, student and District records in accordance with District Policies 8300, 5300, and 1800.

11.0 **Unauthorized Software**. Employees are prohibited from using or possessing any software that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any fees owed to the software owner.

12.0 **Social, Collaborative, Interactive, and Responsive Technologies**. The District supports the use of technologies such as blogs, wikis, podcasts, and online photo management software for educational purposes and communicating with the community. These technologies are considered an extension of the classroom and are approved for use to convey information about District services; promote and raise awareness of the District; and communicate with employees, students, and community members. It is expected that use of District electronic communication resources to participate in activities including, but not limited to, news groups, wikis, blog discussions, and social networking is for bona fide educational purposes.

12.1 The District also acknowledges that employees may choose to utilize these technologies – such as Twitter, MySpace and Facebook on their own time as well as during work time for educational purposes. Personal social networking sites should not be used to encourage inappropriate personal nonprofessional relationships with current or recent students. When utilizing personal social networking sites, District employees are encouraged to consider whether what is posted will impair the employee's professional effectiveness or reputation.

12.2 Employees are responsible for content shared by students when the employee is supervising students engaged in educational activities or sponsoring a student organization pursuant to District Policies 5260, 5650 or 6260.

13.0 **District Makes No Warranties**. The District makes no warranties of any kind, whether expressed or implied, related to the use of District computers and computer systems, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by the District of the content, nor does the District make any guarantee as to the accuracy or quality of information received. The District shall not be responsible for any damages, losses or costs an employee suffers in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the employee's own risk.

LEGAL REFERENCES:
47 U.S.C. §254
47 U.S.C. § 231
20 U.S.C. § 6801 et seq.
C.R.S §22-87-101 et seq.

CROSS REFERENCES:
Code: 1800
Code: 5300
Code: 5620
Code: 5650
Code: 6260
Code: 8300

EXHIBIT
District Policy 4185

EMAIL NOTICES

Employees may append one of the following notices below their signature block in electronic communications as appropriate for the nature and purpose of the message:

NOTICE: This email may contain confidential information considered confidential under the Family Educational Rights and Privacy Act. If you received this in error please notify the sender and delete this message immediately.

or

NOTICE: This email may be a public record subject to disclosure under the Colorado Open Records Act.