

***Superintendent File: GBEE-R***

**RULES FOR EMPLOYEE USE OF DISTRICT INFORMATION TECHNOLOGY**

The intent of these rules is to provide employees with general requirements for utilizing the School District's Information Technology ("District IT") as defined in Policy GBEE. The rules may be supplemented by more specific administrative procedures and rules governing day-to-day management and operation of the computer system.

These rules provide general guidelines and examples of prohibited uses for illustrative purposes, but do not attempt to state all required or prohibited activities by users. Employees who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the principal or appropriate administrator.

Failure to comply with District policy GBEE (**Staff Use of District Information Technology**), these rules, and/or other established procedures or rules governing computer use may result in disciplinary action, up to and including dismissal. Illegal uses of the District IT will also result in referral to law enforcement authorities.

**A. Access to District IT**

The level of access that employees have to District IT is based upon specific employee job requirements and needs.

**B. Acceptable Use**

Employee access to the District IT is provided for administrative, educational, communication, and research purposes consistent with the District's educational mission, curriculum, and instructional goals. General rules and expectations for professional behavior and communication apply to use of District IT.

Employees are to utilize District IT for school-related purposes and performance of job duties. Incidental personal use of District IT is permitted as long as such use does not interfere with the employee's job duties and performance, with system operations, or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures, and rules.

C. Prohibited Use

The employee is responsible for his or her actions and activities involving District IT, and for his or her computer files, passwords, and accounts. General examples of unacceptable uses that are expressly prohibited include, but are not limited to, the following:

1. Any use that is illegal or in violation of other Board policies, including harassing, discriminatory, or threatening communications and behavior; violations of copyright laws or trade secrets; or use of software without proof of proper licensing;
2. Any use involving materials that are obscene, pornographic, sexually explicit, or sexually suggestive;
3. Any inappropriate communications with students or minors;
4. Any use for private financial gain, or commercial, advertising, or solicitation purposes;
5. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate, or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school sponsored organization; to raise funds for any non-school sponsored purpose, whether profit or non-for-profit; or to engage in political activities or campaigns. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students, and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or other appropriate administrator;
6. Any communication that represents personal views as those of the school or District or that could be misinterpreted as such;
7. Downloading or loading software or applications without permission from the system administrator;
8. Opening or forwarding any e-mail attachments (executable files) from unknown sources and/or that may contain viruses;
9. Sending mass e-mails to school users or outside parties for school or non-school purposes without the permission of the system administrator, principal, or designated administrator;

10. Any malicious use or disruption of the District's computers, networks, and Internet services or breach of security features;
11. Any misuse or damage to the District's computer equipment;
12. Misuse of the computer passwords or accounts (employee or other users);
13. Any communications that are in violation of generally accepted rules of network etiquette and or professional conduct;
14. Any attempt to access unauthorized sites;
15. Failing to report a known breach of computer security to the system administrator;
16. Using District computers, networks, and Internet services after such access has been denied or revoked; and
17. Any attempt to delete, erase, or otherwise conceal any information stored on a District computer that violates these rules.

**D. No Expectation of Privacy**

The District retains control, custody, and supervision of all District IT owned or leased by the District. The District reserves the right to monitor all computer and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of school computers, including e-mail messages and stored files. Electronic mail and other electronic records are subject to the Colorado Public Records law, which means that most any e-mail or files sent, received, or stored on the District's computers could be public information and accessible by members of the public.

**E. Confidentiality of Information**

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential. Employees should not use electronic mail for confidential matters or privileged communications, such as student education records, unless appropriate measures are taken to ensure confidentiality and to maintain the appropriate privilege.

F. Staff Responsibilities to Students

Teachers, staff members, and volunteers who utilize District computers for instructional purposes with students have a duty of care to supervise such use to help ensure that students are using computers appropriately and responsibly. Teachers, staff members, and volunteers are expected to be familiar with the District's policies and rules concerning student computer and Internet use and to enforce them. When, in the course of their duties, employees or volunteers become aware of student violations, they are expected to stop the activity and inform the building principal, Chief Technology Officer, or designee.

G. Compensation for Losses, Costs, and/or Damages

The employee shall be responsible for any losses, costs, or damages incurred by the District related to violations of policy GBEE and/or these rules.

H. No Responsibility for Unauthorized Charges, Costs, or Illegal Use

The District assumes no responsibility for any unauthorized charges made by employees, including, but not limited to, credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

I. Proprietary Information

Any information or material including, without limitation, discoveries, ideas, inventions, techniques or processes, that an employee discovers or develops as a result of the employee's employment with the District, whether with the use of District technology or otherwise, shall constitute trade secrets of and be the sole property of the District.

J. Employee Acknowledgement Required

Each employee authorized to access the District's computers, networks, and Internet services is required to sign an acknowledgement form stating that he or she has read policy GBEE and these rules. The acknowledgement form will be retained in the employee's personnel file.

Adopted: May 7, 2002

Repealed by the Board and re-enacted by the Superintendent: August 5, 2003

Revised: \_\_\_\_\_

Douglas County School District Re. 1, Castle Rock, Colorado