



## **GBEE - EMPLOYEE USE OF DISTRICT INFORMATION TECHNOLOGY**

Employee use of District information technology is a privilege, not a right, and is only authorized for work-related purposes. Employee use of District information technology shall be in accordance with this policy, in accordance with governing law and in accordance with other relevant District policies and regulations. Each time an employee uses a District computer or network, the employee shall acknowledge the terms and conditions in this policy that govern the employee's use of District information technology.

Employee authorization to use District information technology may be suspended at any time it is in the District's best interest to do so, as determined by the District in its sole discretion. The District reserves the right to set and revise limits on employee network bandwidth usage and e-mail and file storage on District computers. Employee authorization to use District information technology shall be terminated when the employee ceases to be employed by the District.

As used in this policy, "District information technology" includes District computers, personal communication devices ("PCDs"), e-mail and Internet access. As used in this policy, the term "computer" includes, as applicable, all District computers, computer systems and networks, computer hardware and associated peripheral equipment, and software purchased or developed by the District. As used in this policy, "personal communication device" or "PCD" includes all District cell phones, pagers, personal digital assistants, cameras, audio/video recorders, audio/video players, and other hand-held electronic communication, computing and data storage devices.

### **NO EXPECTATION OF PRIVACY**

Because all employee communications and all related documents, data, software and other information stored on District computers and/or PCDs are authorized only for work-related purposes, employees shall have no expectation of privacy with respect to their use of District information technology. The District reserves the right at any time and without notice to monitor such use and to inspect, copy, review, segregate, store and/or remove any or all communications, documents, data, software and other information related to such use.

### **COMPUTER AND PCD SECURITY**

Employee passwords for logging on to District computers, and for accessing District computers, e-mail and the Internet through other means, shall be carefully guarded to ensure that they are used only by authorized persons. Employees shall not disclose their passwords to anyone, shall not allow another person to gain access to District computers, e-mail or the Internet through the use of their passwords unless expressly

authorized by District technology support personnel, and shall not use another person's password to gain access to District computers, e-mail or the Internet unless expressly authorized by District technology support personnel. The information technology department shall prescribe requirements for password complexity and for the period of time a password may remain in effect before needing to be changed.

Employees shall not leave unattended any computer or PCD without first closing all applications through which the District's confidential student and/or personnel information may be accessed, and shall not leave a District laptop computer, PCD or other portable technology for which they are responsible where it can be taken or used without authorization. Employees are strongly encouraged to password protect their PCDs.

### E-MAIL

After an e-mail is received in an employee's inbox, the employee may retain it in the inbox, save it in another folder or delete it. E-mail deleted from the employee's inbox, saved e-mail folders and sent items folder remains accessible through the employee's account in the "deleted items" folder. The information technology department shall purge employee e-mail on a daily basis one year after it is sent or received in order to help maintain sufficient storage space on the District's system, unless otherwise required by law or District policy, or dictated by District needs.

### RESPONSIBILITIES REGARDING STUDENT INTERNET USE

District employees responsible for classes, programs or activities involving student Internet access shall instruct the students, prior to allowing such access, regarding Internet safety and appropriate online behavior. District employees responsible for classes, programs or activities involving student Internet access shall also assist the students to develop skills to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to search, evaluate and use information appropriate to their educational goals.

### HARDWARE, PERIPHERALS, SOFTWARE AND PROGRAMS

Employees shall not hook up or otherwise attach any computer hardware or peripheral equipment to a District computer unless expressly authorized by District technology support personnel. Employees shall not install, download or run any software or program on a District computer unless expressly authorized by District technology support personnel.

### CONFIDENTIALITY OF STUDENT AND PERSONNEL INFORMATION

Employees shall maintain the confidentiality of all student education records and personally identifiable information developed, sent, received and/or stored through the use of District information technology as required under the Family Educational Rights

and Privacy Act, Colorado Open Records Act, and District Policy JRA/JRC. Employees shall also maintain the confidentiality of all personnel file information developed, sent, received and/or stored through the use of District information technology as required under the Colorado Open Records Act and District Policy GBJ.

Confidential student and personnel information shall only be stored on District computers. Such confidential information shall not be stored on an employee's personally owned computer, PCD or other electronic storage device. Such confidential information shall also not be stored on any electronic transmission or storage technology owned, controlled or operated by a third party. Employees are subject to rules established by the director of information technology governing the types of student, employee and volunteer information that may not be downloaded onto District laptop computers, PCDs and other portable technology.

Employees shall ensure that confidential student and personnel information is disclosed to persons and organizations outside the District only as authorized by law and by District policies and regulations, and that such confidential information is disclosed within the District only to officials having a legitimate educational or supervisory interest in it. Toward these ends, it is imperative that employees use District information technology correctly and carefully to protect against the unauthorized disclosure of confidential student and personnel information.

#### RETENTION AND INSPECTION OF ELECTRONIC RECORDS

Employees shall ensure that all District electronic records for which they are responsible are retained in accordance with the record retention requirements specified in District Policy EHB. Such electronic records not protected by confidentiality or privilege, as provided by law, are subject to inspection and copying by members of the public under the Colorado Open Records Act and District Policy KDB. Electronic student education records are subject to inspection by a student's parent/guardian, and by other persons and organizations, as provided under the Family Educational Rights and Privacy Act and District Policy JRA/JRC.

#### PROHIBITED USES

Employees shall not use District information technology to generate, send, receive or store communications, documents, data, software or other information that:

- contains sexually oriented content or pornography, in either written or picture form, that may be reasonably perceived as having the purpose or effect of stimulating erotic feelings or appealing to prurient interests;
- directs profanity, obscenities or vulgar language toward another person or classification of persons;
- promotes violence or advocates unlawful acts;

- concerns the purchase or manufacture of weapons, controlled substances, or items that it is not lawful to acquire and/or own;
- harasses, threatens or promotes violence against another person or classification of persons;
- concerns the commercial purchase or sale of goods and/or services, or any commercial transaction or advertising related to the employee's personal interests or profit;
- constitutes plagiarism;
- defames another person or classification of persons;
- violates another person's confidentiality, or discloses information regarding which another person has a reasonable expectation of privacy;
- involves impersonation or electronic transmission through an anonymous remailer;
- involves unauthorized access to District computers, computer files, e-mail accounts, e-mail files, or Internet sites;
- involves unauthorized use or downloading of software, files or data;
- violates federal, state or local law, including but not limited to criminal law and trademark, copyright or patent law;
- violates District policy or regulation;
- interferes with the normal operation or use of District computers, e-mail or Internet access, or otherwise disrupts District operations;
- interferes with a school's ability to provide educational opportunities to students.

#### CONSEQUENCES FOR POLICY VIOLATION

Employees found to be in violation of this policy shall be subject to suspension or revocation of use privileges, and to discipline up to and including termination of employment.

Adopted by Superintendent: March 1, 2010  
 Revised by Superintendent: October 31, 2011

LEGAL REFS:

20 U.S.C. 1232g

C.R.S. 22-9-109

C.R.S. 24-72-201 et seq.

CROSS REFS:

EHA, District Information Technology

EHB, Records Retention

GBJ, Personnel Records and Files

JRA/JRC, Student Records/Release of Information on Students

KDB, Public Inspection and Copying of District Records