JS - STUDENT USE OF DISTRICT INFORMATION TECHNOLOGY

Student use of District information technology is a privilege, not a right, and is only authorized for education-related purposes. Student 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 a student uses a District computer or network, the student shall acknowledge the terms and conditions in this policy that govern the student's use of District information technology.

Student 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 student network bandwidth usage and e-mail and file storage on District computers. Student authorization to use District information technology shall be terminated when the student ceases to be enrolled in a District school or program.

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 all District computers, computer systems and networks, computer hardware and associated peripheral equipment, and software purchased, licensed or developed by the District. As used in this policy, "personal communication device" or "PCD" includes all District tablets, cameras, audio/video recorders, audio/video players, and other hand-held electronic communication, computing and data storage devices.

Students may be issued District laptop computers and/or PCDs to be used at school and away from school, which may be conditioned on the payment of a charge for District insurance covering such laptop computers and/or PCDs. Intentional or reckless student acts and omissions that result in damage or loss of District laptop computers and/or PCDs may result in loss of the privilege of being issued a District laptop computer and/or PCD.

NO EXPECTATION OF PRIVACY

Because all student communications and all related documents, data, software and other information stored on District computers and/or PCDs are authorized only for education-related purposes as part of the District's instructional program, students shall have no expectation of privacy with respect to their use of District information technology and Internet access. 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

Student 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. Students shall not disclose their passwords to anyone besides their parent/guardian, 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 a building technology coordinator or 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 a building technology coordinator or District technology support personnel. The executive director of information technology shall prescribe requirements for password complexity and for the period of time a password may remain in effect before needing to be changed.

Students 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. Students shall password protect their PCDs.

STUDENT SAFETY

Students shall not disclose their names or other personally identifiable information such as photographs, home addresses or telephone numbers in connection with their individual use of the Internet through District computers and/or PCDs. Students shall not disclose information that might allow another person to locate them in connection with their individual use of the Internet through District computers and/or PCDs, and shall not arrange face-to-face meetings with persons individually met on the Internet via e-mail or through other electronic communications.

E-MAIL

After an e-mail is received in a student's inbox, the student may retain it in the inbox, save it in another folder or delete it. E-mail deleted from the student's inbox, saved e-mail folders and sent items folder remains accessible through the student's account in the "deleted items" folder. The information technology department shall purge student e-mail at the end of each school year 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.

INTERNET

Technology protection measures that block or filter Internet material that is obscene, child pornography or otherwise harmful to minors, as provided by law, shall be utilized

on all District computers and PCDs through which students may gain Internet access. 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. The District may monitor students' online activity to verify that they are safely and appropriately using the Internet. Despite these protections, it is possible that a student might encounter inappropriate material through Internet access using the District's computers, PCDs and/or network. If this occurs, the student shall immediately back out of the site and notify a responsible District employee.

HARDWARE, PERIPHERALS, SOFTWARE AND PROGRAMS

Students shall not hook up or otherwise attach any hardware or peripheral equipment to a District computer or PCD unless expressly authorized by a building technology coordinator or District technology support personnel. Students shall not directly or indirectly modify or circumvent the operating condition set by the information technology department on any District computer or PCD unless expressly authorized by a building technology coordinator or District technology support personnel.

PROHIBITED USES

Students 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, bullies, threatens or promotes violence against another person or classification of persons;
- concerns the purchase or sale of goods and/or services, or any transaction or advertising related to the student's personal interests or profit;

- constitutes plagiarism;
- defames another person or classification of persons;
- violates another person's confidentiality rights, 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

Students found to be in violation of this policy shall be subject to consequences that may include the suspension or revocation of use privileges, detention, and suspension or expulsion from school.

Adopted by Board: April 13, 2010, effective July 1, 2010
Revised by Board: June 12, 2012, effective July 1, 2012
Revised by Board: April 28, 2015, effective July 1, 2015
Revised by Board: May 28, 2019, effective July 1, 2019

LEGAL REFS:
47 U.S.C. 254(h)
C.R.S. 22-87-101 et seq.

CROSS REFS:
EHA, District Information Technology
EHB, Records Retention
GBEE, Employee Use of District Information Technology
JKDA/JKEA, Grounds for Suspension/Expulsion of Students
JRA/JRC, Student Records/Release of Information on Students