JS - STUDENT USE OF DISTRICT INFORMATION TECHNOLOGY

District information technology supports the education of all students and is only authorized for education-related purposes. Student use of District information technology shall be in accordance with this policy, governing law, and other relevant District policies and regulations. A student agrees to follow the terms and conditions of this policy each time a student uses a District device, service, or network.

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 usage, bandwidth, storage, and other usage parameters as determined to be necessary by the chief technology officer or designee. Student authorization to use District information technology will be terminated when the student ceases to be enrolled in a District school or program. Retention of student data derived from such use shall be handled in accordance with the District's records and retention policies and procedures.

Definitions

As used in this policy, these terms have the following meanings:

- **"District information technology"** means District computers, technology devices , and provisioned software tools and services, including email, curriculum resources and internet access.

- **"District technology device" ("DTD")** means all District purchased and issued tablets, cameras, audio/video recorders, audio/video players, and other hand-held electronic communication, computing and data storage devices. Computing devices include all District computers, laptops, computer systems and networks, computer hardware and associated peripheral equipment, including software purchased, licensed or developed by the District and installed or utilized on the device.

- **"Personal technology device" or "PTD"** means any privately-owned portable technology device, including, but not limited to, cell phones, tablets, laptops, personal locators/GPS monitoring devices, cameras, wearables (watches), ~~and~~ audio and/or video recorders and players, and all other hand-held electronic communication and data storage devices. PTD use is addressed in District Policy JICJ – Student Possession and Use of Personal Technology Devices.

- **"Proprietary"** means when content is owned by someone or something else, through a trademark, patent, or a copyright.
- **"Academic dishonesty"** means engaging in a practice in relation to schoolwork

that does not meet the requirements of the work, where the practice is not disclosed. It includes any material misrepresentation, concealment, or omission as to how the work was completed, such as use of materials not permitted for a test.

- **"Plagiarism"** means representing that work that is not the original creation of the student's is a student's own work. Plagiarism is a type of academic dishonesty.

Students may be issued DTDs 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 DTDs, unless the student qualifies for free or reduced lunch. Intentional or reckless student acts and omissions that result in damage or loss of DTDs may lead to loss or modification of the student's access to a DTD. School sites must work with students who have, for disciplinary reasons, restricted access to student technology to ensure they retain appropriate access to educational resources.

No Expectation of Privacy

DTDs are owned by the District and are intended solely for educational purposes. Students have no expectation of privacy when using District information technology. The District reserves the right to monitor, inspect, copy, review, isolate, store and/or remove (at any time and without notice) all usage of District information technology, including all internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received/created through District information technology remains the property of the District. Students will retain the authorship of any content they create via the use of District information technology.

Computer, Tools and Services Security

Student passwords for logging on to District computers, and for accessing District information technology, must be carefully guarded to ensure that they are used only by authorized persons. Students must not disclose their passwords to anyone besides their parent/caregiver, must not allow another person to gain access to District information technology through the use of their passwords unless expressly authorized by District technology support personnel, and must not use another person's password to gain access to District information technology unless expressly authorized by District technology support personnel. The chief technology officer or designee will prescribe requirements for password complexity and for the period of time a password may remain in effect before needing to be changed.

Students must not leave unattended any DTD or PTD if used to access District information technology without first locking or logging off of all applications through which the District's confidential student and/or personnel information may be accessed, and must not leave a DTD where it can be taken or used without authorization.

Students must password protect their DTDs and PTDs if used to access District information technology.

Email

After an email is received in a student's inbox, the student may retain it in the inbox, save it in another folder or delete it. Email 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 may purge student email at the end of each school year, unless otherwise required by law or District policy, or as 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, will be utilized on all District computers and PTDs 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 will 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, PTDs and/or network. If this occurs, the student shall immediately back out of the site and notify a District employee.

Hardware, Peripherals, Software and Programs

Students may not connect or otherwise attach any hardware or peripheral equipment to a District computer or DTD unless expressly authorized by District technology support personnel. Students shall not directly or indirectly modify or circumvent the operating conditions set by the Information Technology Department on any District computer or DTD unless expressly authorized by District technology support employees.

Artificial Intelligence

The District acknowledges that some student use of Artificial Intelligence (AI) tools may enhance the District's commitment to high-quality learning. Students are only permitted to use AI tools on assignments when clearly stated in the assignment or specified by the teacher. Students should cite their use of AI anytime they engage in its use. If a student is unsure whether AI can be used on an assignment, they should ask their teacher. Intentional misuse of AI on an assignment may constitute plagiarism and academic dishonesty.

In any use of AI, students should be mindful that AI tools are prone to “hallucinations,” false answers/information, or outdated, misleading and/or biased information. Students should always verify information provided by AI tools using reliable sources such as textbooks, scientific papers and reputable websites.

Students should not upload or input any personal, confidential, proprietary, or sensitive information into any AI tool accessed through District information technology. Examples include passwords and other personal information such as names, images of themselves, or social security, credit card or bank account numbers.

Specific acceptable and unacceptable uses of AI tools may vary based on new technological developments and students must follow the guidance of District administrators and classroom teachers.

Prohibited Uses

Students must not use District information technology to generate, send, receive or store communications, documents, data, images, video, software or other information that:

- Threatens the safety of themselves or others.
- Contain 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 (appealing to prurient interests);
- Direct profanity, obscenities or vulgar language toward another person or classification of persons;
- Promote violence or advocate unlawful acts;
- Concern the purchase or manufacture of weapons, controlled substances, or items that are not lawful to acquire or own;
- Harass, bully, threaten, defame, or promote violence against another person or any classification of persons under District Policy AC – Nondiscrimination/Equal Opportunity;
- Constitute plagiarism or other forms of academic dishonesty;
- Violate another person’s confidentiality rights or disclose information regarding which another person has a reasonable expectation of privacy;
- Involve impersonation or electronic transmission through an anonymous proxy;
- Involve unauthorized access to District information technology;
- Involve unauthorized use or downloading of software, files or data;

- Violate federal, state or local law, including but not limited to criminal law and trademark, copyright or patent law;

- Violate District policy or regulation;

- Interfere with the normal operation or use of District information technology, or otherwise disrupt District operations; or

- Interfere with a school's ability to provide educational opportunities to students.

Consequences for Policy Violation

Students found to be in violation of this policy will be subject to consequences that may include the suspension, modification, 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
Revised by Board:

Cross References:
AC – Nondiscrimination/Equal Opportunity
EHA - District Information Technology
EHB - Records Retention
GBEE - Employee Use of District Information Technology
JICJ – Student Possession and Use of Personal Technology Devices
JKDA/JKEA - Grounds for Suspension/Expulsion of Students
JRA/JRC - Student Records/Release of Information on Students

Legal References:
47 U.S.C. 254(h) (telecommunication services for educational providers)
C.R.S. 22-87-101 et seq. (Children's Internet Protection Act)