JS
STUDENT USE OF INFORMATION TECHNOLOGY RESOURCES

Adopted: May 4, 2010
Amended: June 19, 2012
Adopted: December 11, 2012
Adopted December 10, 2013

This policy shall govern student use of District Information Technology Resources (DITR), regardless of whether such use occurs on or off District property, and regardless whether use occurs by means of direct connection, telephone line or other common carrier, or by means of any other type of connection or electronic communication, including, but not limited to, wire, fiber, infrared, or wireless media.

For purposes of this policy, DITR shall include hardware, software and data that is owned, leased, licensed, or otherwise kept and maintained by the District for the purpose of accessing, storing, downloading/uploading, recording, sending, receiving, posting, distributing, delivering, displaying or printing electronic or digital information, curriculum, messages, records, mail, files or data. DITR shall include, but is not limited to, District computers, computer systems and computer peripherals, electronic tablets, iPads, e-readers, smartphones and similar devices, District local and wide-area computer networks and servers, District e-mail and other electronic communication systems, District-hosted or District-sponsored internet access, websites and connectivity, and the equipment and software programs or packages associated with such access, connectivity, systems and equipment.

Declaration of Purposes

The Board of Education finds that technological advances have fundamentally altered the way in which information is retrieved, conveyed and transmitted in our society. Such changes require educators to adapt and integrate appropriate new technology into the learning process to facilitate, support and enhance delivery of curriculum and as tools and resources to educate and to inform. The District is committed to make available for student use DITR in schools for the following purposes—

- To provide access to relevant and appropriate academic information and resources available on the internet and through electronic communication and data storage systems;
- To allow students to participate in on-line or electronic curriculum or distance learning activities as needed or appropriate;
- To consult and communicate with other students and individuals for educational purposes;
- To conduct academic or educational research;
- To engage in activities requiring students to think critically, analyze information, write clearly, and use problem-solving skills;
- To practice and develop computer and research skills that are necessary for continued education or entry into the workforce upon graduation; and
- To foster intellectual curiosity and shape positive student attitude toward lifelong learning.

Regulated Access and Use

Access and use of DITR is reserved for District students and staff for the limited purposes set forth above, and shall not be open or available for use by the general public. Except as provided in Board policy regarding student publications, no District-owned or sponsored website or other component of DITR shall constitute or be established or maintained as a public forum.

Blocking or filtering obscene, pornographic and harmful information

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The Board recognizes that it is impossible to predict with certainty what information students may access or obtain. Nevertheless, the district shall take reasonable steps to protect students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, as defined by the Board. Technology protection measures that block or filter material and information that is obscene, pornographic or otherwise harmful to minors, as defined by the Board, shall be installed or implemented with respect to each DITR component or device that allows for access to the Internet by a minor . Such technology protection measures may be relaxed or disabled for student use only for bona fide research purposes authorized by and under the direct supervision of a district staff member.

Students shall report access to material and information that is obscene, child pornography, harmful to minors or otherwise in violation of this policy to the supervising staff member. If a student becomes aware of other students accessing such material or information, he or she shall report it to the supervising staff member.

No expectation of privacy

DITR and its components, including computers, servers and systems, are owned by the district and are intended for educational purposes at all times. Students shall have no expectation of privacy when using them or when accessing or using the Internet or electronic communications by means of DITR. The district reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of DITR, including district computers and computer systems and the files contained therein, including all Internet and electronic communications access and transmission/receipt of materials and information. All files, data, material and information stored, accessed, received, downloaded or uploaded through or by means of DITR shall remain the property of the district.

Security

DITR shall be administered in a manner that places a high priority on security and student safety in connection with student use of DITR, especially in connection with on-line activities. Students who identify a security problem, such as a suspected computer virus, while using the Internet or electronic communications must immediately notify a system administrator. Students should not demonstrate, circulate or download the problem to other users.

In addition, students shall not:

—Disclose or share passwords except as authorized by school officials, attempt to obtain, modify or use another person's password or any other identifier, attempt to log on to the Internet or other DITR as a system administrator, or log in through another user’s account;

—Gain or attempt to gain unauthorized access to another user’s files or data, to District file servers

or other DITR devices or components, or to third party file servers.

—Read, alter, delete or copy or intercept electronic communications of other system users, or attempt to engage in such activities.

—Use "hacking" software or other tools to hack or compromise DITR security measures or components, or introduce, install or upload spyware, computer viruses or malware to or with DITR or to any device, component or network within DITR.

Safety

Students shall not reveal or transmit to third parties not employed by the district any personal social security numbers, home addresses, phone numbers, photographs or other personally identifiable information about themselves while using DITR to access the Internet or other electronic communications, and shall not be required to do so by district staff members. Without first obtaining permission of the supervising staff member, students shall not use their last name or any other information that might allow another person to locate or identify him or her. Students shall not use DITR to arrange face-to-face meetings with persons met on the Internet or through electronic communications.

Vandalism

Vandalism of DITR is prohibited. For purposes of this policy, vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse, reconfigure or disrupt operation of any DITR, including, but not limited to, any network within the school district or any network connected to the Internet, operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or district-owned software or hardware. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Unauthorized software

Students shall not download or install any software, mobile app, shareware, freeware onto DITR servers, drives or disks without prior authorization from the supervising staff member or District Technology Services personnel. Students are prohibited from using DITR to use, share, install, download or otherwise obtain or distribute any copyrighted software, music, video or data files that has been downloaded or is otherwise in the user's possession unlawfully or without appropriate license from the copyright owner.

Other Unauthorized and Unacceptable Uses

Students shall use DITR in a responsible, efficient, ethical and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of DITR cannot be specifically described in policy. However, at minimum, students are prohibited from using DITR to violate or facilitate or carry out any conduct that is in violation of the Code of Student Conduct. In addition,

no student shall use DITR to access, create, transmit, retransmit or forward material or information:

1. that 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;
2. that uses inappropriate or profane language that is likely to be offensive to others in the school community;
3. that contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion;
4. that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the district's policies against discrimination, bullying and other violent or aggressive behaviors;

5. for personal profit, financial gain, advertising, political campaigns or other private or commercial purposes not within the scope of the declared educational purposes of DITR set forth in this policy;
6. that copies, reproduces or plagiarizes the work of another without authorization from the author or owner of the work;
7. that is knowingly false or could be construed as intending to purposely damage another person's reputation;
8. in violation of any federal or state law or other district policy or regulation, including but not limited to, the District's policy regarding use of copyrighted material;
9. that impersonates another or transmits through an anonymous remailer; or
10. that accesses fee services without specific permission from the system administrator.

The Board directs and authorizes the Superintendent to develop appropriate additional rules and regulations governing acceptable use of DITR as may be necessary to effectuate the intent and purposes of this policy. Such regulations shall include reasonable procedures, requirements and restrictions and conditions regarding such use in order to—

(a) assure that students use DITR in a responsible, efficient, ethical and legal manner, and only for educational purposes as set forth above;

(b) detect and prevent the use of DITR in connection with the receipt or transmittal of inappropriate or harmful material via Internet, electronic mail, or other forms of direct electronic communications;

(c) detect and prevent unauthorized access to or use of DITR;

(d) maintain and enforce standards for acceptable use of DITR as set forth in this policy;

(e) address privacy issues, including unauthorized online disclosure, use, or dissemination of personal identification information or other private facts regarding any person; and to

(f) comply with the Children's Internet Protection Act and other applicable laws.

Online Activity Education and Monitoring

Students using or permitted to use DITR shall receive education designed to develop their intellectual skills needed to discriminate among information sources, to enhance their ability to identify information appropriate to their age and developmental levels and to evaluate and use information to meet their educational goals. Such education shall also address appropriate online behavior, and include specific instruction regarding interaction with other individuals on social networking websites, in chat rooms and through other platforms for direct electronic communication, and regarding cyberbullying awareness and response. Students shall have specifically defined objectives and search strategies prior to using DITR to access material and information on the Internet and/or through electronic communications.

The district will make reasonable efforts to monitor the online activities of students to verify that students are using DITR responsibly and safely. The Superintendent may develop a plan to identify and coordinate specific monitoring activities of administrators, teachers and other staff members. Staff members assigned to supervise student use of DITR shall exercise due diligence in monitoring student online behavior and activities, and shall receive training in Internet and electronic communications safety and appropriate monitoring methods, provided funding is available for such training.

Upon request, parents shall be afforded an opportunity to observe student use of the Internet and electronic communications in schools.

Student use is a privilege

Student use of the Internet and electronic communications is a privilege, not a right. The district may deny, revoke or suspend a student's access to or use of DITR at any time, in which case the student's accounts or files may be closed or locked.

The building principal may deny or restrict access to or use of DITR with respect to any student whose use of DITR poses an identifiable security risk, whose disciplinary record demonstrates repeated misconduct involving the Internet, electronic communications or other information technology resources, or whose privilege to access or use such resources was revoked or restricted by the school or other institution at which the student was last enrolled or placed.

Students shall take responsibility for their own use of DITR and for understanding the acceptable and unacceptable uses of such tools, especially when accessing Internet or participating in electronic communications, to avoid contact with inappropriate material or information. Compliance with this policy and the Code of Student Conduct is a condition of such use. Failure to comply with this policy shall be grounds for revocation or suspension of any or all DITR privileges, and may result in school disciplinary action, including suspension or expulsion. In the event unlawful conduct has occurred or is suspected, the violation may also be reported to law enforcement.

Students and parents/guardians may be required to sign, as a condition of granting or continuing access and privileges to use DITR, a document affirming the student's acceptance of responsibility for acceptable and responsible use of DITR and acknowledging receipt of this policy and its implementing regulations, if

any.

No warranties or endorsement

It is impossible to predict with certainty what information students might locate or be exposed to through the Internet or otherwise obtain or be exposed to while using DITR. The District makes no guarantee or warranty as to the accuracy, quality or appropriateness of information obtained by or through use of DITR, nor does the availability of information by means of DITR imply or endorsement or approval by the District of the content of such information. The district shall not be responsible for any damages, losses or costs a student suffers in using DITR, including damages, losses or costs incurred from loss of data and service interruptions, as well as losses or damages caused by unauthorized use, misdeliveries, non-deliveries, or exposure to harmful information. Use of any information obtained via the Internet and electronic communications is at the student's own risk.

LEGAL REFS.: 47 U.S.C. 254(h) *(Children's Internet Protection Act of 2000)*
47 U.S.C. 231 *(Children's Online Privacy Protection Act of 1998)*
20 U.S.C. 6801 *et seq.(Elementary and Secondary Education Act)*
C.R.S. 22-87-101 *et seq. (Children's Internet Protection Act)*
47 U.S.C. § 254(h)(5)B) (*Protecting Children in the 21st Century Act)*

CROSS REFS.: AC, Nondiscrimination/Equal Opportunity
JICDA, Code of Student Conduct
JICJ, Student Use of Cell Phones and Other Personal Electronic Devices