Mesa County Valley School District 51

JS-R

STUDENT USE OF INFORMATION TECHNOLOGY RESOURCES

Related: JS
Superintendent Effective Date: May 4, 2010
Revised: February 29, 2012
Revised: December 18, 2012
Revised December 11, 2013

Purpose

This regulation implements Board policy JS by setting forth specific procedures, requirements and restrictions and conditions governing student use of District Information Technology Resources (DITR). 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.

Responsible Use Agreement

Before being granted privileges to use the District's technology, including Internet access, e-mail, computers and networks, all students, unless they are 18 years of age or older, must have an Responsible Use Agreement, Exhibit JS-E ("RUA") signed by a parent or guardian. Students must also sign the RUA if they are in enrolled in Grade 6 or above. All completed RUA forms must be returned to the child's school.

The RUA form will be provided with the school's registration paperwork and may also be obtained by contacting the school's administration. Once a signed RUA has been submitted to the student's school, the RUA is in effect for as long as the student is attending that school. A newly-signed RUA is required when a student is registering to attend one of the District's schools for the first time, is changing schools because of a family move or grade promotion, or is experiencing a change in guardianship. Schools will retain the signed RUA for as long as the student is attending the particular school. For more information about technology use by students, please contact the school's administration.

Access to District Information Technology Resources (DITR)

Student use of DITR is a privilege, not a right. DITR may be used only by students who have been issued network user accounts that are active and have not been denied, closed, locked or suspended. Except as otherwise determined by the building principal in consultation with the Executive Director of Technology Services, a student must meet all of the following requirements to be eligible to receive or maintain an active network user account:

(a) The student has completed and submitted an RUA signed by the student and/or parent/guardian as required above to the school at which DITR will be used; and

(b) The student is not subject to any disciplinary order issued by the District or revoking, suspending, denying prohibiting or restricting access to or use of DITR or any component thereof; and

(c) The student is not subject to any court order, probation or parole condition or restriction in force or effect that prohibits the Student from accessing or using DITR or any component thereof; and

(d) The student's privilege to access or use DITR is not suspended, revoked or denied by the school or building principal or other administrator due to violations of the rules of use set forth in this regulation, or

A student's network user account may at any time be denied, restricted, closed, locked or suspended at the request of the building principal at the school where the student is enrolled. Such request may be made at any time such principal determines that (1) the student is not eligible to receive or maintain an active network user account under the above requirements, (2) that the student has a record of repeated and willful misconduct involving the Internet, electronic communications or other information technology resources, or for other reasons poses an identifiable and significant security risk, or (3) that the student's privilege to access or use such resources was within the past twelve (12) months revoked or restricted by the school or other institution at which the student was last enrolled or placed.

DITR Services and Functions
The District reserves the right to determine the specific DITR services or functions that will be made available for student use, and the nature, extent, speed and types of such DITR services or functions shall be subject to change at any time. Network traffic or systems may be restricted or shut down when computing requirements exceed available capacity, or when necessary to conduct investigations, make repairs, conduct maintenance or install, replace or upgrade DITR hardware, software or systems. The District's technology department shall, if practicable, provide advance notice to schools and student users regarding any anticipated changes or interruptions in DITR services or functions.

The District is not obligated to offer connectivity or to continue user access to any particular online or Internet service or feature. Such decisions are the responsibility of the Executive Director of Technology Services, who shall consider all relevant factors, including, but not limited to, impact on network bandwidth, compatibility with systems in use in the District, and suitability for K-12 educational use. Board policies governing selection of appropriate instructional materials and course content shall be applicable to curriculum and courses delivered by or with DITR. Students shall not be permitted or authorized to enter into any contracts or other agreements with outside agencies, organizations, or businesses offering online services without review and approval of such arrangement by the Executive Director of Technology Services.

Types of DITR services or functions to which students may be provided access through their network user accounts include, but are not limited to:

1. Internet Access –The Internet is a valuable tool for students. When using the Internet for class activities, teachers will select material that is age appropriate and relevant to course objectives. Teachers will determine the appropriateness of the material contained on or accessed through any web site they require or recommend. Teachers will instruct students to research effectively as outlined in District information literacy standards. School staff will teach Internet safety and appropriate use of internet resources. However, the District shall install and maintain software and other technology protection measures that may limit, block, or filter Internet usage or other on-line activities of students. The District shall not be responsible for any unauthorized charges or fees resulting from students accessing the Internet.

2. Electronic Mail (email) –Use of student network accounts for email or other messaging services shall be limited to consultation and communication with other students, staff and third parties for educational purposes. Students may not establish or access commercial or web-based email accounts through DITR unless such accounts are required by the curriculum and meet the requirements for protection of student confidentiality, privacy, and security set forth below.

3. Guest Accounts –Upon the request of a teacher or administrator and with the approval of the Executive Director of Technology Services or his/her designee, guest accounts may be set up for parents or other guests of students for a specific district-related purpose and time period. The use of guest accounts shall be subject to the same policies and regulations as students, and the account privileges of a guest user may be terminated or restricted at any time without notice in the event of noncompliance or expiration of the time period for which the guest account was authorized. A signed RUA is required for an adult guest account and a parent/guardian signature shall be required if the guest account is assigned to a minor.

4. Interactive Web Communications Areas –The District may provide access to interactive communication areas to students only for specifically defined and authorized educational activities. Students may use interactive electronic communication only under direct supervision of a teacher or other designee as approved by the building administrator.

5. Videoconferencing – The District may provide videoconferencing equipment allowing participants to see, hear, and speak with other participants in real time. With the approval of the Executive Director of Technology Services or his/her designee, videoconferencing activities, events or classes at one school or site may be recorded, linked or shared with participants at other schools or sites within or outside the school district.

Monitoring and Investigation of Student Use
To the extent allowed by law and Board policy, the District shall cooperate to the extent permitted by applicable privacy laws and regulations with any investigation by local, state, and federal authorities or Internet service provider(s) concerning or related to the misuse of DITR and/or suspected violation of any applicable laws. Students should have no expectation of privacy regarding the content of electronic files or accounts they create, distribute, maintain, access or use by means of DITR. DITR devices and components, student network user accounts, data and information shall remain the property of the District at all times. For the purposes described in Board Policy JS, the District reserves the right to:

1. Inspect, view, monitor, capture, copy, print and archive any and/or all files, communications, email, web sites, blogs and other student network or on-line activity accessed, created, sent, received, downloaded or uploaded by means of DITR. The District's inspection and monitoring activities may include examination and review of files, devices, server storage space usage, processor and system utilization, and all services and applications provided through the DITR or associated with a student's network user account, including electronic mail, messaging, and other means of electronic communications that currently exist or may exist in the future.
2. Block, filter and restrict access to any Internet sites or functions that are deemed inappropriate or unauthorized in accord with Board policy JS.
3. Limit the amount of storage space allocated to student electronic files and/or email, and remove email and/or files taking up an excessive amount of storage space after a reasonable amount of time.
4. Investigate, track, log, access and report all aspects of DITR used by or accessible to students, including computers, laptops, electronic tablets, iPads, e-readers, smartphones and other hardware.

Parent Involvement
Helping students to understand and comply with Board policy and rules regarding responsible student use of DITR shall be a responsibility that is shared by schools and parents/guardians. Parents/guardians may request in writing that a teacher or school set and convey more stringent standards for their children to follow when using technology, which requests shall be accommodated if practicable. Upon written request submitted by a student's parent/guardian, such student's privilege to or use of DITR may be revoked or restricted in the discretion of building principal or administrator.

Technology Protection Measures
In compliance with the Children's Internet Protection Act (CIPA) and other applicable laws, technology protection measures (which may include blocks or filters) designed to prevent Internet access to inappropriate material shall be installed and utilized with respect to each DITR component or device that allows for access to the Internet by a minor. The District recognizes that it is unlikely that such measures will be effective in screening all inappropriate material. If a student accidentally accesses or witnesses another student accessing material that he or she believes is offensive, obscene, pornographic or otherwise inappropriate, he or she should notify the supervising teacher or other District staff member.

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, but may not be disabled at times when such action could expose other students to material prohibited under CIPA. The District may, from time to time, reconfigure the technology protection measures to best meet the educational and safety needs of the District, and to comply with legal requirements.

Rules of Responsible Use
General rules of school behavior, including the Code of Student Conduct (Board policy JICDA) shall apply to student use of the Internet and DITR. In addition, students shall, as a condition of granting or continuing access and privileges to use DITR, comply with the following additional rules for responsible use:

Students shall NOT—

1. Change computer settings without authorization.
2. Unplug cables or open computer cases, except as directed by a supervising staff member.
3. Place food, beverages, or other liquids near computers.

4. Download, upload, or share music, games, audio, or video files except with teacher permission.
5. Reveal or transmit 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. 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.
6. Forward, post or distribute a message, file or other material that contains social security numbers, home addresses, phone numbers, photographs or other personally identifiable information about other students without such student's written permission.
7. Agree to meet with someone they have met online without their parent's knowledge and approval.
8. Download or install any software, mobile app, shareware, or freeware onto network drives or disks without prior permission of supervising teacher, or the District's technology department.
9. Create, establish or maintain web pages or other ways to advertise or sell products or services and may not offer, provide, or purchase products or services through the use of DITR, except for school-approved activities.
10. Upload, download, or distribute pornographic, obscene, or sexually explicit, photographs, images, videos.
11. Gain or attempt to gain unauthorized access to any District file servers or other DITR devices or components, outside file servers, or go beyond the student's authorized access. It shall be a violation of this rule to log in or attempt to log in to through another person's network user account, or otherwise access or modify another person's files or data.
12. Use DITR to violate any criminal law or to otherwise engage in, support or facilitate illegal acts or activities.
13. Disclose or share passwords except as authorized by school officials, or attempt to obtain, modify or use another person's password or any other identifier, or attempt to log on to the Internet or other DITR as a system administrator.
14. Read, alter, delete or copy or intercept electronic communications of other persons without permission, or attempt to engage in such activities.
15. 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. While on school property or at school activities, students shall not use, possess or distribute any software tools designed to facilitate hacking or compromise a computer or network.
16. Engage in vandalism, unauthorized use of software or any unauthorized or unacceptable uses of DITR as enumerated and described in Board Policy JS.

Students SHALL—

1. Use DITR in a responsible, efficient, ethical and legal manner.
2. Comply with building or classroom rules during or regarding the use of DITR.
3. Protect their passwords against inadvertent or unauthorized disclosure. Students who discover or suspect that someone has discovered or is using their password should contact a responsible staff member or Technology Services (Help Desk) immediately.
4. Use printer resources responsibly.
5. Be polite and respectful to others when communicating with others through District email and other DITR services.
6. Refrain from accessing material that is not relevant to their class assignments or course work, or otherwise wasting time and technology resources
7. Obtain approval from teacher and parents before entering or using chat rooms or social networking sites.
8. Assume that all materials available on the Internet are protected by copyright. Students must not copy, download, forward, or upload any copyrighted material without prior approval of the copyright holder and supervising teacher. Any material obtained from the Internet and included in one's own work must be cited and credited by name or by electronic address or path on the Internet. Information obtained through email or news sources must also be credited as to sources.

9. Immediately notify a system administrator, teacher or other school staff member if he or she identifies a security or safety problem, such as a suspected computer virus, or a message or contact they receive that is inappropriate or makes them feel uncomfortable, while using the Internet or electronic communications. Students should not delete, download, forward or distribute the problem file or message to other users or students until and unless instructed to do so by a staff member.
10. Be encouraged to report on-line harassment, threats, bullying, and other misconduct to a teacher or administrator.

Consequences of Misuse

Failure to follow the rules of use contained in this regulation may result in the temporary or permanent loss or restriction of the student's privilege to use DITR and associated inactivation or closure of the student's network user account. Serious or repeated violations of such rules may also result in disciplinary action under Board Policy JS or other school disciplinary policies and regulations. The District may deny, revoke, or suspend access to District Information Systems or close accounts at any time. Students have the responsibility to respect and protect the rights of every other User in the District and on the Internet/network/software, hardware, peripherals, and other Information Systems equipment.

Intentional unauthorized access to and/or damage to District networks, servers, user accounts, passwords, or other DITR may be punishable under local, state, or federal law. In the event any District staff member or administrator receives information causing him or her to conclude or suspect that a violation of state or federal law has occurred or is occurring in connection with student use of DITR, such suspected violation shall be promptly reported to appropriate law enforcement agencies. To the extent permitted by law, the District will cooperate with local, state, or federal officials in any investigation concerning, or related to, suspected criminal or unlawful activities involving student use of DITR.

Student Use of Third Party Sites

Teachers shall take reasonable steps to protect the confidentiality of student personal information when establishing any relationship with a third-party web site or technology system. Students may establish individual accounts on a third party web site or system for in-school use if the site is on the district approved list of third party resources and teacher guidelines are followed. This list will contain guidelines and restrictions in the use of the specific sites on the list and will be reviewed annually under the direction of the Executive Director, Student Achievement and Growth-Curriculum and Instruction.