MARSHALL PUBLIC SCHOOLS

SERIES 300
INSTRUCTION

363.2

ACCEPTABLE USE OF TECHNOLOGY AND COMMUNICATION RESOURCES BY STUDENTS

Purpose statement:
Students are reminded that the use of district technology, including the Internet and other communication resources, is a privilege, not a right. District technology is defined as any device or software owned by the district, or contracted for use by the district, for the specific and limited purpose of supporting the educational mission of the district that allows communications between individuals or groups, including but not limited to: desktop and portable computers; modems and software used to connect over a telephone line to the district's computer network; file servers, web servers, virtual servers, and print servers; projection devices, software applications, and the variety of electronic devices, such as cell phones, pagers, and personal tablet devices, digital assistants that electronically transmit information between users and provide wireless connectivity for accessing and utilizing district resources.

The primary purpose of providing access to district resources is to enhance teaching and learning, thereby better preparing students for success in life and work. This access is provided to increase communication within the District, enhance productivity and assist users in improving their skills. Access is also provided to assist in the sharing of information with the local community, including parents/guardians, social service agencies, government agencies and businesses.

Security measures:
Each authorized user will be issued identification and personalized passwords in order to access the system. Students must have a signed Student Internet Acceptable Use Consent Form (Board Rule 363.2; Board Exhibit 363.2) indicating acceptance of the policies, rules, and procedures on file in order to receive district approval to access district technology resources. Students are prohibited from providing access to others with the use of their identification and password, and are subject to discipline up to and including loss of privileges related to the use of district technology and network access, and may include criminal penalties, should they provide prohibited access.

Privacy rights:
Users should have no expectation of personal privacy in connection with their usage of such District network and other technology resources. Network supervision and security maintenance may require monitoring of directories, messages, or Internet activity. The District retains the right to monitor, access, and review all messages or information, e.g., files, created, received or sent over, or stored on, District technology and communication networks at all times and without notice in order to determine compliance with acceptable use of the District's resources.

Individuals using district technology resources must have approval to use any or all district technology resources.

Some material on the Internet may contain items that are inaccurate or potentially offensive to some people. Although efforts are being taken to minimize student exposure to inappropriate material through the use of an Internet filter, it is ultimately the responsibility of parents and guardians of minors to set and convey standards that their children should follow when using electronic resources like the Internet. Parent/guardian permission shall be required before a student is allowed to use the Internet at school for educational purposes.

1. General Use Rules

a. Students must adhere to the same standards of conduct expected and required in the classroom.
b. All students have the same opportunity to use the equipment, software, network resources and e-mail. Students shall use these computer resources for academic activities only.
c. To preserve security, students should protect their computer passwords and change them periodically. If a password is improperly disclosed, it will be changed immediately.
d. Designated school personnel may conduct random checks of students who are on-line with the Internet or other computer network for the purpose of ensuring compliance with Board policy and the acceptable use rules.

2. Rules of Network Safety and Acceptable Use

All students are expected to abide by the generally accepted rules of network safety and acceptable use. These rules include the following:

a. All use of the Internet or other communication resources must be in support of education and research and consistent with the policies, goals and objectives of the District. The use of online social networking sites, such as chat rooms, wikis, blogs, forums and other applications (e.g. Web 2.0) will be allowed only in controlled, staff-supervised settings, and for valid school-related and/or instructional purposes. All other uses are prohibited. "Social networking," as used in this policy, means establishing, maintaining, posting to, or otherwise participating in an electronic community on websites, blogs, or through accounts on social networking sites.
b. Online social networking sites are an extension of the classroom. Therefore, students must adhere to classroom and building rules and procedures as outlined in student handbooks. Appropriate language must be used at all times. Students will not swear, use vulgarities or any other inappropriate language, bully, or engage in activities that are prohibited under state or federal law.
c. Transmission of any material in violation of any United States or state regulation is prohibited. This includes but is not limited to copyrighted material, threatening, inflammatory, derogatory, libelous or obscene material or images, child pornography, or material protected by trade secret. In addition, the transmission of any material that causes disruption to the learning environment or is harmful to minors is not allowed.

d. Students will not tamper with hardware or software, destroy someone else's computer files, copy or download computer data, software or programs without authorization, create anonymous postings, or intercept and/or disclose electronic communication, including e-mail, while it is in transit.
e. Harassment, discrimination, defamation, "cyber-bullying" and vandalism will not be tolerated. Harassment is behavior toward another based on any personal characteristic, such as, but not limited to, race, sex, or disability, that substantially interferes with a student's school performance or creates an intimidating, hostile or offensive environment. For purposes of this policy, harassment is defined as the persistent annoyance of another user or the interference of another user's work. Defamation is an intentional publication of a false communication that injures another person's reputation or good name. Vandalism is defined as any malicious attempt to harm, modify or destroy data of another user or network equipment. "Cyber-bullying" is defined as using technology to intimidate, humiliate, manipulate, mislead, threaten or otherwise harm another person. Vandalism and harassment will result in cancellation of student Internet and computer lab privileges and may result in other disciplinary action consistent with established school and District policies.
f. While on-line, students are prohibited from sharing personal information about themselves or others that implicates their personal or financial security or is otherwise in violation of this policy, including, but not limited to, personal computer passwords, names, addresses, phone numbers, social security numbers, credit card information and so on.
g. Students will not use the networks in such a way that would disrupt the use of the networks by other users.
h. District technology networks, including e-mail systems, shall not be used for private business ventures, personal gain, political promotion or campaigning.
i. All material and information accessible via the network, including computer software, should be assumed to be copyrighted, the private property of the owner, and should not be copied or used by others without permission of the owner of the material or information or authorized as "fair use" under federal copyright laws. The same laws and guidelines apply for use or copying of information on the Internet or other on-line sources as apply to use and reproduction of printed hard copies of the same information.
j. Use of any information obtained via the Internet is at the student's own risk. The Marshall Public School District specifically denies any responsibility for the accuracy or quality of information obtained through its technology and communication network resources. All students need to consider the source of any information they obtain, and consider how valid that information may be. It is the student's responsibility not to initiate access to inappropriate materials.
k. Guidance will be provided to students about what they should do if they receive any electronic transmission that they feel is inappropriate or makes them feel uncomfortable. In such situations, they are expected to inform school staff.
l. E-mails received from an unknown person should be deleted and not opened.
m. Spamming and/or chain e-mail letters are not allowed. School staff should be contacted when any form of chain letter, virus alert, or other mass e-mail message (spam) is received.

n. Students' file directories should be cleaned out when a file is no longer needed. All student files should be deleted at the end of the school year.

3. Personally-owned Laptops and Other Computing or Communications Devices

a. A personally-owned laptop computer, handheld computer or other computing or communications device may be connected to the Internet only through the District's public wireless network, which allows filtered web-only access to the Internet. Connecting a laptop to a non-networked device such as a projector or SMARTboard is allowed for instructional purposes only.
b. The laptop computer, handheld computer, or other computing or communications device is to be used in compliance with District policies and rules. Any violation of such policies or rules may result in the exclusion of the device from school and/or discipline of the person who has violated the policy and/or rule.
c. Any staff or student who brings a laptop computer, handheld computer or other computing/communication device to school must use it as an instructional tool and only for the school curriculum. It may not be used as an entertainment system. Students must turn off and put away a personal laptop, handheld computer or other computing device when directed by a staff member.
d. If a cellphone is found or is confiscated, the person recovering the phone is not authorized to view contents of the phone. District protocol requires staff to turn the device in to the office. The district administrative staff or agent and/or a law enforcement representative are the only persons authorized to view the contents.
e. The District may examine personal computers and other electronic devices and search their contents if there is a reason to believe that school policies, including this policy, rules or regulations or laws have been violated. Individuals have no expectation of privacy in the use of the District's wireless network or Systems and such use is subject to being monitored.
f. Neither students nor staff are required to bring personal electronic property to school. The District accepts no responsibility for the loss, theft or damage of personal property brought to school by staff or students. Any laptop computer, handheld computer, or other electronic device is the sole responsibility of the staff member or student who brought the device to school.

4. Penalties for Improper Use

Violation of these rules, applicable state and federal laws or posted classroom, school, and district rules will result in loss of network and computer lab privileges and/or other disciplinary action as defined in the appropriate handbooks, up to and including suspension or expulsion.

Violations could also lead to referral to legal authorities for prosecution under applicable laws.

Access to district technology resources may be denied or terminated if one is identified as a repeat offender, or if an initial offense is of sufficient severity to justify immediate denial of access to district technology resources.

The Marshall School District recognizes the need to provide technology to further the educational goals and mission of the District. The Internet and communication resources provide unique educational opportunities and challenges to a learning community. Licensed staff and library media specialists have a professional responsibility to blend thoughtful use of such information with the curriculum and to provide guidance and instruction to students in the appropriate use of such resources. All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber-bullying awareness and response.

Staff shall adhere to the guidelines for instructional resources and the goals for the selection of instructional materials contained in Board policy.

In compliance with federal law requirements, an Internet filtering device shall be used on all District computers that access the Internet in an effort to protect against access to visual depictions that are obscene, child pornography and materials harmful to minors.

Legal References:

Cross References: Board Policy 363.2 Acceptable Use of Technology and Communication Resources by Students
Board Exhibit 363.2 Student Internet Acceptable Use Consent Form
Board Policy 443.72 Cyber Bullying

Date of Adoption: December 16, 2009

Date of Revision: July 17, 2013