

ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS AND RESOURCES (M)

2361 ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS AND
RESOURCES (M)

M

The Board shall develop a technology plan that effectively uses electronic communication to advance and promote learning and teaching. This system of technology shall be used to provide local, Statewide, national and global communications opportunities for staff and pupils. Educational technology shall be infused into the district curriculum to maximize pupil achievement of the Core Curriculum Content Standards/Common Core State Standards.

Purpose

To support its commitment to providing avenues of access to the universe of information available, the district's system of electronic communication shall include access to the Internet for pupils and staff.

Limitation of Liability

The Internet constitutes an unregulated collection of resources that change constantly, so it is not possible to totally predict or control the resources that users may locate. The Board cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the Board shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. Nor shall the Board be responsible for financial obligations arising through the unauthorized use of the system.

District Rights and Responsibilities

The computer system is the property of the district, and all computer software and hardware belong to it. Therefore, the district retains the right to monitor all access to and use of the Internet.

The Board designates the Superintendent as the coordinator of the district system. He/she shall recommend to the Board of Education qualified staff persons to ensure provision of individual and class accounts necessary for access to the Internet, designation of quotas for disk usage on the system, establishment of a document retention schedule, establishment of a virus protection process and coordination of other activities as required to maintain the system.



ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS AND RESOURCES (M)

Each Principal shall coordinate the district system in his/her building by approving all activities for that building; ensuring that teachers receive proper training in the use of the system; ensuring that pupils are adequately supervised when using the system; maintaining executed user agreements; and interpreting this acceptable use policy at the building level.

Access to the System

This acceptable use policy shall govern all use of the system. Sanctions for pupil misuse of the system shall be included in the disciplinary code for pupils, as set out in Board Policy. Employee misuse may result in appropriate discipline in accord with the collective bargaining agreement and applicable laws and regulations.

The Board shall ensure the acquisition and installation of blocking/filtering software to deny access to certain areas of the Internet.

Internet Safety Protection

As a condition for receipt of certain Federal funding, the school district shall be in compliance with the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and has installed technology protection measures for all computers in the school district, including computers in media centers/libraries. The technology protection must block and/or filter material and visual depictions that are obscene as defined in Section 1460 of Title 18, United States Code; child pornography, as defined in Section 2256 of Title 18, United States Code; are harmful to minors including any pictures, images, graphic image file or other material or visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or depicts, describes, or represents in a patently offensive way, with respect to what is suitable for minors, sexual acts or conduct; or taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

This Policy also establishes Internet safety policy and procedures in the district as required in the Neighborhood Children's Internet Protection Act. Policy 2361 addresses access by minors to inappropriate matter on the Internet and World Wide Web; the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; unauthorized access, including "hacking" and other unlawful activities by minors online; unauthorized disclosures, use, and dissemination of personal identification information regarding minors; and measures designed to restrict minors' access to materials harmful to minors.



ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS AND RESOURCES (M)

Notwithstanding blocking and/or filtering the material and visual depictions prohibited in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act, the Board shall determine other Internet material that is inappropriate for minors.

In accordance with the provisions of the Children's Internet Protection Act, the Superintendent of Schools or designee will develop and ensure education is provided to every pupil regarding appropriate online behavior, including pupils interacting with other individuals on social networking sites and/or chat rooms, and cyberbullying awareness and response.

The Board will provide reasonable public notice and will hold one annual public hearing during a regular monthly Board meeting or during a designated special Board meeting to address and receive public community input on the Internet safety policy - Policy and Regulation 2361. Any changes in Policy and Regulation 2361 since the previous year's annual public hearing will also be discussed at a meeting following the annual public hearing.

The school district will certify on an annual basis, that the schools, including media centers/libraries in the district, are in compliance with the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act and the school district enforces the requirements of these Acts and this Policy.

World Wide Web

All pupils and employees of the Board shall have access to the Web through the district's networked or stand alone computers. An agreement shall be required. To deny a child access, parent(s) or legal guardian(s) must notify the Building Principal in writing.

Individual E-mail Accounts for District Employees

District employees shall be provided with an individual account e-mail account for professionally related communications.

System Limits

Users shall access the system only for educational, professional or career development activities. This applies to discussion group mail lists, instant message services and participation in Internet "chat room" conversations.

Users shall check e-mail frequently and delete messages promptly.



ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS AND RESOURCES (M)

Supervision of Pupils

Pupil use of the Internet shall be supervised by qualified staff.

District Website

The Board authorizes the Superintendent to establish and maintain a district website. The purpose of the website will be to inform the district educational community of district programs, policies and practices.

Individual schools and classes may also establish websites that include information on the activities of that school or class. The Building Principal shall oversee these websites.

The Superintendent shall publish and disseminate guidelines on acceptable material for these websites. The Superintendent shall also ensure that district and school websites do not disclose personally identifiable information about pupils without prior written consent from parent(s) or legal guardian(s). Consent shall be obtained on the form developed by the State Department of Education. "Personally identifiable information" refers to pupil names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

Parental Notification and Responsibility

The Superintendent shall ensure that parent(s) or legal guardian(s) are notified about the district network and the rules governing its use. Parent(s) or legal guardian(s) shall sign an agreement to allow their child(ren) to have an individual account. Parent(s) or legal guardian(s) who do not wish their child(ren) to have access to the Internet must notify the Principal in writing.

Pupil Safety Practices

Pupils shall not post personal contact information about themselves or others. Pupils should not engage in any kind of unauthorized personal contact from individuals they meet online. Attempts at contact from such individuals shall be reported immediately to the staff person monitoring that child's access to the Internet. Personal contact information includes but is not limited to names, home/school/work addresses, telephone numbers, or personal photographs.

Prohibited Activities



ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS AND RESOURCES (M)

Users shall not attempt to gain unauthorized access to the district system or to any other computer system through the district system, nor shall they go beyond their authorized access. This includes attempting to log in through another individual's account or accessing another's files.

Users shall not deliberately attempt to disrupt the district's computer system performance or destroy data by spreading computer viruses, worms, "Trojan Horses," trap door program codes or any similar product that can damage computer systems, firewalls, servers or network systems.

Users shall not use the district system to engage in illegal activities.

Users shall not access material that is profane or obscene, that advocates illegal acts, or that advocates violence or hate. Inadvertent access to such material should be reported immediately to the supervising staff person.

Users shall not plagiarize material that is available on the Internet. Plagiarism is presenting another's ideas/words as one's own. Users shall not infringe on copyrighted material and shall follow all dictates of copyright law and the applicable policies of this district.

Prohibited Language

Prohibited language applies to public messages, private messages, and material posted on web pages.

Users shall not send or receive messages that contain obscene, profane, lewd, vulgar, rude, inflammatory, or threatening language.

Users shall not use the system to spread messages that can reasonably be interpreted as harassing, discriminatory or defamatory.

System Security

Users are responsible for their accounts and should take all reasonable precautions to prevent unauthorized access to them. In no case should a user provide his/her password to another individual.

Users shall immediately notify the supervising staff person or data processing department if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems.



ACCEPTABLE USE OF COMPUTER NETWORKS/COMPUTERS AND RESOURCES (M)

Users shall not install or download software or other applications without permission of the supervising staff person.

Users shall follow all district virus protection procedures when installing or downloading approved software.

Privacy Rights

Users shall respect the privacy of messages that they receive and refrain from reposting messages without the approval of the sender.

Users shall not publish private information about another individual.

Implementation

The Superintendent shall prepare regulations to implement this policy.

The Superintendent shall ensure that curriculum in the arts, including both visual and performing, are developed appropriately for each grade level.

Adopted: 17 December 2013

