Book: FHSD REGULATIONS

Section: 6000 INSTRUCTIONAL SERVICES/ 6300 Learning Commons, Media and Technology Services

Title: Network and Internet Usage

Code: 6320

Status: Active

Adopted: May 1, 2010

Last Revised: June 2, 2016

Privileges
The use of District technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. Staff and students are only allowed to conduct electronic network-based activities which are classroom or workplace related.

Personal Responsibility
Access to research via electronic resources requires students and staff members to maintain consistently high levels of personal responsibility. The existing rules found in the District's Behavioral Expectations policy (Board Policy/Regulation 2610) as well as employee handbooks clearly apply to students and staff members using electronic resources for research or communication.

Personal Technology
The District is committed to providing technology for use by students and staff. The District also realizes that there are often not enough devices available for students and staff to assist in their work. Students and staff are allowed to use their personal devices for the purposes of completing district and classroom work. Personal technology devices are defined as any electronic device personally owned by students or staff, including laptops, tablets, or smart phones. Staff and students will be allowed to connect to the District Wi-Fi network will be have their internet access filtered on these devices.

Students and staff are not required to bring their own personal technology devices to school.

District-owned Technology Off-site

District-owned technology may be used away from school and the District network. The policies and regulations that apply while using district-owned technology on district property apply when these same devices are used away from school.

Network Etiquette

Students and staff members are expected to abide by the generally accepted rules of electronic network etiquette. These include, but are not limited to, the following:

1. Students and staff members are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others.

2. Students and staff members are expected to use appropriate language; language which uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.

3. Students and staff members may not use District's electronic network in such a manner that would damage, disrupt, or prohibit the use of the network by other users.

Internet Access

In compliance with the Children's Internet Protection Act ("CIPA"), 47 U.S.C.§254, the District uses technological devices designed to filter and block the use of any District computer with Internet access to retrieve or transmit any visual depictions that are obscene, portray child pornography, are determined to be "harmful to minors" as defined by CIPA, and material which is otherwise inappropriate for students.

Content Filtering/Monitoring

The District shall use filtering, blocking or other technology to protect students and staff from accessing Internet sites that contain any form of communication that is obscene, pornographic or harmful in nature. Any attempt to bypass or disable the District's filtering/blocking device will be considered a violation of the Acceptable Use Guidelines. The District shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA).

Due to the dynamic nature of the Internet, sometimes Internet websites and web material that do not fall into these categories are blocked by the filter. In the event that a student or staff member feels that a website or web content has been improperly blocked by the District's filter and this website or web content is appropriate for access by students or staff, the process described below should be followed:

1. Follow the process prompted by the District's filtering software and submit an electronic request for access to a website by entering an email address and specifying the reason for the request. If a user prefers to remain anonymous, the requester should use 123anonymous in the email address field), or:

2. Submit a request, whether anonymous or otherwise, to the District's superintendent/designee.

3. Requests for access shall be granted or denied within three business days. If a request was submitted anonymously, persons should attempt to access the website requested after three days. If a properly formatted email address is used, individuals will be notified via email within three business days if the request is granted or denied.

4. Appeal of the decision to grant or deny access to a website may be made in writing to the Board of Education. Persons who wish to remain anonymous may mail an anonymous request for review to the Board at the District's Central Office, stating the website that they would like to access and providing any additional detail the person wishes to disclose.

5. In case of an appeal, the Board will review the contested material and make a determination. The Board's decision in this matter is final.

6. Material subject to the complaint will not be unblocked pending this review process.

In the event that a District student or employee feels that a website or web content that is available to District students through District Internet access is obscene, portrays child pornography, is determined to be "harmful to minors" as defined by CIPA or otherwise inappropriate for District students, the process set forth in Regulation 6241 should be followed.

Adult users of a District computer with Internet access may request that the “technology protection measures" be temporarily disabled for lawful purposes so long as the use is not otherwise inconsistent with this Regulation.

Internet Safety/Privacy
In compliance with the CIPA, all District students will annually receive Internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response. Such training will include Internet, cell phones, text messages, chat rooms, email and instant messaging programs. (See also Policy 6116 – State Mandated Curriculum – Human Sexuality).

1. Users may not reveal their or any other individual’s personal information (e.g., personal address, personal phone numbers, last names) during electronic communications. Students should only use first name and last name initial when posting electronic communications.

2. Staff members may not reveal students' personal information (e.g., personal address, personal phone numbers, last names) during electronic communication without parental permission.

3. Users should not assume a legal expectation of privacy when using District technology resources, including but not limited to, e-mail, chat, blogs, social networking, and wiki. Users should understand that all communication and information is public when transmitted via the network and may be viewed by other users. The system administrators may access and read any electronic communication on a random basis.

4. All users will be instructed on the dangers of sharing personal information about themselves or others over the Internet and are prohibited from sharing such information unless authorized by the District. Student users shall not agree to meet with someone they have met online without parent approval and must promptly disclose to a teacher or other staff member any message the user receives that is inappropriate or makes the user feel uncomfortable.

5. Use of the District's electronic network for unlawful purposes is prohibited and will not be tolerated.

Passwords
To comply with the acceptable use of District electronic resources, students and staff members must demonstrate respect for, and protection of, password/account code security, as well as restricted databases files and information banks. Personal passwords/account codes may be created to protect students and staff members utilizing electronic resources to conduct research or complete work.

These passwords/account codes shall not be shared with others, nor shall students or staff members use another party’s password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects staff members and students from wrongful accusation of misuse of electronic resources or violation of District policy and state or federal law. Students or staff members who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse.
Students and staff are prohibited from using the save password feature on web pages or applications that provide the user access to personally-identifiable or confidential information.

Students will be required to change their password one time per year and staff will be required to change their password twice per school year. Passwords must be complex in nature. Complex passwords consist of eight (8) or more characters made up by using three (3) of the following four (4) categories: upper case, lower case, special character and numbers. Passwords may only be reused every fourth (4th) time.

Acceptable Use
The use of the District technology and electronic resources is a privilege, which may be revoked at any time. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage to or theft of system hardware or software; alteration of system software; placement of unlawful information, computer viruses or harmful programs on, or through the computer system;

entry into restricted information on systems or network files in violation of password/account code restrictions; repeated instances of inappropriately disclosing user password/account code; violation of other users' right to privacy; using another person's name to send or receive messages on the network;; and use of the network for personal gain, commercial purposes, or engaging in political activity not allowed by Board policy.

Staff members may not claim personal copyright privileges over files, data or materials developed in the scope of their employment, nor may students or staff members use copyrighted materials without the permission of the copyright holder. The connections represented by the Internet allow users to access a wide variety of media. Even though it is possible to download most of these materials, students and staff shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

Access to an electronic mail (e-mail) system(s) is a privilege and is provided to assist students and staff members in the acquisition of knowledge and for efficient communication with others. Any e-mail system provided by the District is designed solely for educational and work-related purposes. E-mail files are subject to review by District and school personnel. Chain letters and "chat rooms" are not allowed, with the exception of those bulletin boards or "chat" groups that are created by teachers for specific instructional purposes or by staff members for specific work-related communication in accordance with the District's content/filtering monitoring guidelines.

Students or staff members who engage in investigatory activities commonly described as "hacking" are subject to loss of privileges and District discipline, as well as the enforcement of any District policy or state and/or federal laws that may have been violated. Hacking may be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the District, a business, or any other governmental agency obtained through unauthorized means.

Students and staff members are not permitted to obtain, download, view or otherwise gain access to materials which may be deemed unlawful, harmful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions.

Authorized District personnel reserve the right to remove files, limit or deny access, and refer staff members or students violating the Board policy for other disciplinary action.

Services

While the District provides access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The District may not be held responsible for any damages including loss of data as a result of delays, non-delivery or service interruptions caused by the information system or the user's errors or omissions. The use or distribution of any information that is obtained through the information system is at the user's own risk. The District specifically denies any responsibility for the accuracy of information obtained through Internet services.

Security

The Board recognizes that security on the District's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privileges creates a risk for all users of the information system.

The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems which arise from the users sharing their account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to the information system.

Users are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the classroom teacher or system administrator.

Closed Forum

The District is to be considered a closed forum and any District technology, including, but not limited to, computers, e-mail, websites, and cell phones are not to be used as public forms of expression.

Vandalism of the Electronic Network or Technology System

Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the District information service, or the other networks that are connected to the Internet. This includes, but is not limited to, the uploading or creation of computer viruses, the alteration of data or the theft of restricted information. Any vandalism of the District electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

Consequences

The consequences for violating Regulation 6320, commonly referred to as the District's Acceptable Use Guidelines include, but are not limited to, one or more of the following:

1. Suspension of District network privileges;
2. Revocation of network privileges;
3. Suspension of Internet access;
4. Revocation of Internet access;
5. Suspension of computer access;
6. Revocation of computer access;
7. School suspension;
8. Expulsion; or
9. Staff disciplinary action up to and including dismissal.

May 2010
Revised June 2013
Revised February 2015
Revised December 2015
Revised June 2016