Iraan-Sheffield Independent School District

Acceptable Use Policy

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

Availability of Access

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

Use by the Members of the Public

Access to the District's electronic communications system, including the Internet, shall also be made available to members of the public, in accordance with administrative regulations. Such use may be permitted so long as the use:

1. Imposes no measurable cost on the District; and
2. Does not unduly burden the District's computer or network resources.

Members of the public who are granted access shall be required to comply with all District rules, regulations, and policies governing appropriate use of the system.

Acceptable Use

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and use agreements, consistent with the purposes and mission of the District and with law and policy governing copyright. [See EFE]

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Non-compliance may result in suspension of access or termination of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct] Violations of law may result in criminal prosecution as well as disciplinary action by the District.

Internet Safety

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Control student’s access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities; and
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.

Filtering

Each District computer with Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children’s Internet Protection Act and as determined by the Superintendent or designee.

The Superintendent or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent or designee, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.

Monitored Use

Electronic mail transmissions and other use of the electronic communications system by students and employees are not private and may be monitored at any time by designated District staff to ensure appropriate use.

Intellectual Property Rights

Students shall retain all rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created for its use by a student even when the author is no longer a student of the District

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created for its use by an employee even when the author is no longer an employee of the District.

Disclaimer of Liability

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

The Superintendent or designee will oversee the District's electronic communications system.

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical use of this resource.

Consent Requirements

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the owner(s) or individual(s) the owner specifically authorizes may upload copyrighted material to the system.

No original work created by any District student or employee will be posted on a web page under the District's control unless the District has received written consent from the student (and the student's parent) or employee who created the work. [See CQ(Exhibit)]

No personally identifiable information about a District student will be posted on a web page under the District's control unless the District has received written consent from the student's parent.

System Access

Access to the District's electronic communications system will be governed as follows:

1. District employees will be granted access to the District’s computer system upon completing the necessary AUP form and receiving the signature of their immediate supervisor. An employee must submit an approved AUP form only once during their tenure of employment.

2. Students in grades K-5 will be granted access to the District's system by their teachers, as appropriate.

3. Students in grades 6-12 will be assigned individual accounts that will include home directories. Internet accounts will be activated for students upon receipt of a signed AUP. Students may not access Web-based e-mail accounts.

4. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to all or part of the District's system.

Technology Coordinator Responsibilities

The technology coordinator for the District's electronic communications system (or campus designee) will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.

2. Ensure that all users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. Agreements will be maintained on file in the principal's office.

3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.

4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.

5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.

6. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.

7. Set limits for data storage within the District's system, as needed.

8. Provide and administer an Internet filtering system.

Individual User Responsibilities On-Line Conduct

The following standards will apply to all users of the District's electronic information/communications system:

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.

2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.

3. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.

4. Students may not distribute personal information about themselves or others by means of the electronic communication system.

5. System users must purge electronic mail in accordance with established retention guidelines.

6. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.

7. System users may not upload programs to the system. System users may download public domain programs for their own use or may noncommercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.

8. System users may not send or post messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

9. System users may not purposefully access materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

10. System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.

11. System users may not waste District resources related to the electronic communications system.

12. System users may not gain unauthorized access to resources or information.

13. Teachers may purchase from personal funds software for their classrooms for use on school computers. The teacher must keep all original program disks and licenses with the respective computer. By signing this Acceptable Use Policy, the teacher guarantees that he/she is in full compliance with the licensing requirements of the software.

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment or data or data of another user of the District' system, or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences. [See DH, FN series, FO series, and the Student Code of Conduct]

Forgery Prohibited

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail or other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

Information Content/Third-Party Supplied Information

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material.

A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher.

A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District' system and will be subject to disciplinary action in accordance with the Student Code of Conduct.
An employee knowingly bringing prohibited materials into the school's environment will be subject to disciplinary action in accordance with District policies. [See DH]

Participation in Chat Rooms, Newsgroups and Web-based message services

Student participation in Internet-based chat rooms and newsgroups is permissible only for school projects under appropriate supervision of the classroom teacher. Employee participation in Internet-based chat rooms and news groups will be the responsibility of the employee’s immediate supervisor.

Development of Web Pages

The technology coordinator (or his designee) will maintain District Web pages for informational and education purposes. Through the appropriate curriculum, students will be encouraged to develop Web pages that, upon review and approval by the respective campus principal and the technology coordinator, will be posted to an appropriate area of the District's Web page.

Network Etiquette

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in all capital letters are the computer equivalent of shouting and are considered rude.

2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.

3. Pretending to be someone else when sending/receiving messages is considered inappropriate.

4. Transmitting obscene messages or pictures is prohibited.

5. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

Termination/ Revocation of System User Account

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

Disclaimer

The District's system is provided on an "as-is, as-available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.