

Randolph Field Independent School District Internet Safety Plan

The school district has technology protection measures for all computers in the school district, including computers in media centers/libraries, that block and/or filter visual depictions that are obscene, child pornography and harmful to minors as defined in the Children's Internet Protection Act. The school district will certify that schools in the district including media centers and libraries are in compliance with the Children's Internet Protection Act.

Compliance measures contained within this plan address the following:

Access by Minors to Inappropriate Matter on the Internet and World Wide Web

1. Users will not use the district system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, special exception may be made for hate literature if the purpose of such access is to conduct research AND both the teacher and the parent approve access. District employees may access the above material only in the context of legitimate research.
2. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access in a manner specified by their school. Students should immediately notify teachers. Teachers and staff should immediately notify building administration. Building administration should immediately notify supervisor of technology. This will protect users against an allegation that they have intentionally violated the acceptable use policy.
3. The fact that the filtering technology has not protected against access to certain material shall not create the presumption that such material is appropriate for users to access. The fact that the filtering software has protected access to certain material shall not create the presumption that the material is inappropriate for users to access.

Randolph Field ISD will provide student access to Internet resources only in supervised environments and has taken steps to lock out objectionable areas to the extent possible, but potential dangers remain.

Safety and Security of Minors when using Electronic Mail, Chat Rooms, and other Forms of Direct Electronic Communications and Unauthorized Disclosures

1. Student users will not post or share contact information about themselves or other people. Personal contact information includes the student's name together with other information that would allow an individual to locate the student, including, but not limited to, parent(s) name(s), home address/ location, work address/location, or phone number.

Securing the Learning Environment

2. Elementary and middle school students will not disclose their full name or any other personal contact information for any purpose.
3. High school students will not disclose personal contact information, except to education institutes for educational purposes, companies or other entities for career development purposes, or with specific staff approval.
4. Students will not disclose names, personal contact information, or any other private or personal information about other students under any circumstances. Students will not forward a message that was sent to them privately without permission of the person who sent them the message.
5. Students will not agree to meet someone they have met online.
6. Students will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable. Students should not delete such messages until instructed to do so by a staff member.

Unauthorized Access, Including "Hacking" and other Unlawful Activities by Minors Online

1. Security on any computer network is a high priority, especially when the network involves many users. If a user feels he/she can identify a security problem on the computer network, the user must notify a network administrator or building level administrator. The user should not inform individuals other than network or building administrators of a security problem.
2. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person.
3. Passwords to the network should not be easily guessed by others, nor should they be words that could be found in a dictionary.
4. Attempts to log in to the network using either another user's account or as a network administrator could result in termination of the account. Users should immediately notify a network administrator if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any user identified as a security risk will have limitations placed on usage of the network or may be terminated as a user and be subject to other disciplinary action.
5. Users will not attempt to gain unauthorized access to the district system or to any other computer system through the district system, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purpose of "browsing".

Securing the Learning Environment

6. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.
7. Users will not use the district system to engage in any illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person, etc.
8. Users will not attempt to access Web sites blocked by district policy, including the use of proxy services, software, or Web sites.
9. Students will not attempt to access non-instructional district systems, such as student information systems or business systems.
10. Users will not use sniffing or remote access technology to monitor the network or other user's activity.
11. Users will not use any wired or wireless network (including third party internet service providers) with equipment brought from home. Example: The use of a home computer on the network or accessing the Internet from any device not owned by the district.
12. Users will not use district equipment, network, or credentials to threaten employees, or cause a disruption to the educational program.
13. Users will not possess published or electronic material that is designed to promote or encourage illegal behavior or that could threaten school safety, using the Internet or Web sites at school to encourage illegal behavior, or threatening school safety.
14. Users will not use the district equipment, network, or credentials to send or post electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

Technology Protection Measure (Internet Filtering)

The district has selected a technology protection measure (Internet filtering) for use with the district Internet system. The filtering technology will always be configured to protect against access material that is obscene, illegal (i.e. child pornography) and material that is harmful to minors, as defined by the Children's Internet Protection Act. The district or individual schools may, from time to time, reconfigure the filtering software to best meet the educational needs of the district or schools and address the safety needs of the students.

The filter may not be disabled at any time that students may be using the district Internet system, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. The filter may be disabled during non-student use time for system administrative purposes.

Securing the Learning Environment

Filtering technology has been found to inappropriately block access to appropriate material. To ensure that the implementation of the technology protection measure is accomplished in a manner that retains district control over decision making regarding the appropriateness of material for students; does not unduly restrict the educational use of the district Internet system by teachers and students; and ensures the protection students' constitutional right to access to information and ideas, authority will be granted to the supervisor of technology and to the network administrator to temporarily or permanently unblock access to sites blocked by the filter.

To temporarily unblock a site, the authorized individual must review the content of the site, outside of the presence of any student, prior to allowing access to the site by a student.

Reports of all instances of temporary unblocking will automatically be forwarded to the supervisor of technology.

If an unauthorized individual believes that the blocked site should be permanently unblocked, a recommendation will be forward to the supervisor of technology or the network administrator. The supervisor of technology will make a decision to permanently unblock access to the site or may delegate the decision to the network administrator.

Teachers may request that a blocked site be temporarily or permanently unblocked.

Board Policy and Acceptable Use Guidelines

Related information is contained in Board Policy and the Acceptable Use Guidelines of the district.