

South Iron R-I School District

Acceptable Use of Technology Policy

This Acceptable Use Policy is a summary of official Board policies designated EHB and EHB-R. The content and meaning are essentially identical, but all users will be held accountable to all Board policies.

Principles

The South Iron R-I School District recognizes the educational and professional value of electronics-based information technology, both as a means of access to enriching information and as a tool to develop skills that students need.

The district's technology exists for the purpose of maximizing the educational opportunities and achievement of district students. The professional enrichment of the staff and Board, and increased engagement of the students' families and other patrons of the district are assisted by technology, but are secondary to the ultimate goal of student achievement.

Use of technology resources in a disruptive, manifestly inappropriate or illegal manner impairs the district's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to the district's technology resources. Development of students' personal responsibility is itself an expected benefit of the district technology program.

User Identification and Network Security

Use of the district's technology resources is a privilege, not a right. No student, employee, or other potential user will be given an ID, password or other access to district technology if he/she is considered a security risk by the superintendent or designee.

Users must adhere to district policies, regulations, procedures, and other district guidelines. All users shall immediately report any security problems or misuse of the district's technology resources to an administrator or teacher.

User Agreement

Unless authorized by the superintendent or designee, all users must have an appropriately signed *User Agreement* on file with the district before they are allowed access to district technology resources. All users must agree to follow the district's policies, regulations and procedures.

Privacy

A user does not have a legal expectation of privacy in the user's electronic mail or other activities involving the district's technology resources.

The district may examine all information stored on district technology resources at any time. The district may monitor employee and student technology usage. Electronic communications, all data stored on the district's technology resources, and downloaded material, including files deleted from a user's account, may be intercepted, accessed or searched by district administrators or designees at any time.

In addition, all users must recognize that they do not have a legal expectation of privacy in any e-mail use activities involving the district's technology. A user ID with e-mail access, if granted, is provided to users of this district's network and technology resources only on condition that the user consents to interception or access to all communications accessed, sent, received or stored using district technology in his or her *User Agreement*.

Content Filtering and Monitoring

The district will monitor the on-line activities of minors and operate a technology protection measure ("filtering/blocking device") on all computers with Internet access, as required by law. The filtering/blocking device will protect against access to visual depictions that are obscene, harmful to minors and child pornography, as required by law. Parents are advised, however, that none of these devices can be guaranteed to be completely effective. Because the district's technology is a shared resource, the filtering/blocking device will apply to all computers with Internet access in the district. Evasion or disabling of the filtering/blocking device installed by the district, including attempts to evade or disable, is a serious violation of district policy.

Damages

All damages incurred by the district due to the misuse of the district's technology resources, including the loss of property and staff time, will be charged to the user. District administrators have the authority to sign any criminal complaint regarding damage to district technology.

No Warranty/Availability/No Endorsement

The district makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. The district's technology resources are available on an "as is, as available" basis. Administrators of computer resources may suspend access to and/or availability of the district's technology resources to diagnose and investigate network problems or potential violations of the law or district policies, regulations and procedures.

The district is not responsible for loss of data, delays, non-deliveries, mis-deliveries or service interruptions. The district does not guarantee the accuracy or quality of information obtained from the Internet, or use of its technology resources. Access does not include endorsement of content or the accuracy of the information obtained.

Rules and Responsibilities

The following rules and responsibilities will be followed by all users of the district technology resources:

- a. Applying for a user ID under false pretenses is prohibited.
- b. Using another person's user ID and/or password is prohibited unless authorized by the district.
- c. Sharing one's user ID and/or password with any other person is prohibited unless authorized by the district.
- d. A user will be responsible for actions taken by any person using the ID or password assigned to the user.
- e. Deletion, examination, copying or modification of files and/or data belonging to other users without their prior consent is prohibited.
- f. Mass consumption of technology resources that inhibits use by others is prohibited.
- g. Unless authorized by the district or building administrator, non-educational Internet usage is prohibited.
- h. Use of district technology for soliciting, advertising, fund-raising, commercial purposes or for financial gain is prohibited, unless authorized by the district.
- i. Accessing fee services without permission from an administrator is prohibited. A user who accesses such services without permission is solely responsible for all charges incurred.
- j. Users are required to obey all laws, including criminal, copyright, privacy, defamation and obscenity laws. The school district will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using district technology in violation of any law.
- k. Accessing, viewing or disseminating information using district resources, including e-mail or Internet access, that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, pervasively indecent or vulgar, or advertising any product or service not permitted to minors is prohibited.
- l. Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of district staff for curriculum-related purposes.
- m. Accessing, viewing or disseminating information using district resources, including e-mail or Internet access, that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g. threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful school regulations is prohibited.
- n. Any use which has the purpose or effect of discriminating or harassing any person or persons on the basis of race, color, religion, sex, national origin, ancestry, disability, age, pregnancy, or the violation of any person's rights under applicable laws is prohibited.
- o. Any unauthorized, deliberate, or negligent action, which damages or disrupts technology, alters its normal performance, or causes it to malfunction is prohibited, regardless of the location or the duration of the disruption.
- p. Users may only install and use properly licensed software, audio or video media purchased by the district or approved for use by the district. All users will adhere to the limitations of the district's technology licenses. Copying for home use is prohibited unless permitted by the district's license, and approved by the district.
- q. At no time will district technology or software be removed from the district premises, unless authorized by the district.
- r. All users will use the district's property as it was intended. Technology or technology hardware will not be moved or relocated without permission from an administrator. All users will be held accountable for any damage they cause to district technology resources.
- s. All damages incurred due to the misuse of the district's technology will be charged to the user. The district will hold all users accountable for the damage incurred and will seek both criminal and civil remedies, as necessary.

- t. Unauthorized use of any computer/media equipment or accounts is prohibited. Students may not access the Internet without a teacher or other district staff member present in the room. Students may not access e-mail during school hours except during scheduled times and in designated locations before and after school unless authorized by a staff member for class assignments.
- u. Computers/media equipment must not be marked on, colored on, handled roughly, hit, or in any way defaced, altered or abused.
- v. Horseplay of any kind is not allowed around computer/media equipment.
- w. Students and community users may not have food or beverages around any computer/media equipment.
- x. Users may not move or unplug any computer/media equipment not adjust computer equipment controls without permission from the equipment supervisor.
- y. Students and community users may only access computer programs that have been placed on their menus by the system administrator or supervisor. After consulting with the district technology coordinator, exceptions may be approved by a district administrator or the administrator of the building in which the computer is located.
- z. Any attempted violation of district policy, regulations or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation.

Technology Security and Unauthorized Access

All users shall immediately report any security problems or misuse of the district's technology resources to a teacher or administrator.

No person will be given access to district technology if he/she is considered a security risk by the superintendent or designee.

- a. Use of district technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.
- b. Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.
- c. The unauthorized copying of system files is prohibited.
- d. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology are prohibited.
- e. Any attempts to secure a higher level of privilege on the technology resources without authorization are prohibited.
- f. The introduction of computer "viruses," "hacking" tools, or other disruptive/destructive programs into a school computer, the school network, or any external networks are prohibited.
- g. Users are not to add, remove or alter computer passwords, security measures, configuration settings or monitoring devices without authorization.

On-Line Safety - Disclosure, Use, and Dissemination of Personal Information

- a. All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet.
- b. Student users are prohibited from sharing personal information about themselves or others over the Internet, unless authorized by the district.
- c. Student users shall not agree to meet with someone they have met on-line without parental approval.
- d. A student user shall promptly disclose to his/her teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable.
- e. Users shall receive or transmit communications using only district-approved and district-managed communication systems. For example, users may not use messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the district or building administrator.
- f. All district employees will abide by state and federal law, Board policies, and district rules when communicating information about personally identifiable students.
- g. Employees shall not transmit confidential student information using district technology, unless designated for that use. Employees will take precautions to prevent negligent disclosure of student information or student records.
- h. No curricular or non-curricular publication distributed using district technology will include the address, phone number or e-mail address of any student without permission.

Electronic Mail

A user is responsible for all electronic mail ("e-mail") originating from the user's ID or password.

- a. Forgery or attempted forgery of e-mail messages is illegal and prohibited.
- b. Unauthorized attempts to read, delete, copy or modify e-mail of other users are prohibited.
- c. Students may not access e-mail during school hours except during scheduled times and in designated locations before and after school unless authorized by a staff member for class assignments.

- d. Users are prohibited from sending unsolicited electronic mail to more than 200 addresses per message, per day, unless the communication is a necessary, employment-related function, or an authorized publication.
- e. All users must adhere to the same standards for communicating on-line that are expected in the classroom, and consistent with district policies, regulations and procedures.

Employee Users

Authorized employees may use the district's technology resources for reasonable, incidental personal purposes as long as the use does not violate any provision of district policy, regulation or procedure, hinder the use of the district's technology for the benefit of its students or waste district resources. Any use which jeopardizes the safety, security or usefulness of the district's technology is considered unreasonable. Any use which interferes with the effective and professional performance of the employee's job is considered unreasonable.

All employees must model the behavior expected of students, exhibit the same judgment as expected of students and serve as role models for students. Because computers are shared resources, it is not appropriate for an employee to access, view, display, store, print or disseminate information via district resources, including e-mail or Internet access, which students or other users could not access, view, display, store, print or disseminate, unless authorized by the district.