Part B – Internet Safety Policy

Acceptable Use Policy

Board Policy 645.13
INSTRUCTION

Access to Electronic Networks

Electronic networks, including the Internet, are a part of the District's instructional program in order to promote educational excellence by facilitating resource sharing, innovation, and communication. The Superintendent or designee shall develop an implementation plan for this policy and appoint a system administrator.

The District is not responsible for any information that may be lost, damaged or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. Furthermore, the District will not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Curriculum

The use of the District's electronic networks shall (1) be consistent with the curriculum adopted by the District as well as the varied instructional needs, learning styles, abilities, and developmental levels of the students, and (2) comply with the selection criteria for instructional materials and library-media center materials. Staff members may, consistent with the Superintendent;s implementation plan, use the Internet throughout the curriculum.

The District's electronic network is part of the curriculum and is not a public forum for general use.

Technology Protection Measure

The district technology coordinator periodically monitors and reviews the access logs generated by the filtering system, SmartFilter DA through the Illinois Century Network. This filtering system blocks visual depiction of:

a. Obscenity
b. Child pornography
c. Materials harmful to minors

Any violations to the district's AUP/Internet Safety Policy are reported to the district superintendent.

Monitoring online activities

Teachers are instructed to continuously monitor and supervise all students, in the classroom or in a lab setting, when they are participating in an Internet activity to ensure that they are not engaged in inappropriate activities such as trying to bypass district filters in order to access obscene web sites. They should also monitor students to be sure they are not participating in other unlawful activities such as hacking into servers or administrative computers in order to change grades or obtain personal information on other students or staff. Teachers should also limit student use of personal e-mails and participation in on-line chat rooms or other Internet sites where personal information could be disclosed.

Acceptable Use

All use of the District's electronic network must be (1) in support of the education and/or research, and be in furtherance of the District's stated goal, or (2) for a legitimate school business purpose. Use is a privilege, not a right. Students and staff members have no expectations of privacy in any material that is stored, transmitted, or received via the District's electronic network or District computers. General rules for behavior and communications apply when using electronic networks. The District's *Acceptable Use Policy* contains the appropriate uses, ethics, and protocol. Electronic communications and downloaded material, including files deleted from a user's account but not erased, may be monitored or read by District officials.

Internet Safety

Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are (1)obscene, (2)pornographic, or (3)harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Building Principal or designee. The Principal or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide researchor other lawful purposes, provided the person receives prior permission from the Principal or system administrator. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Limiting student and adult access to inappropriate matter as well as restricting access to harmful materials;
2. Student and adult safety and security when using electronic communications;
3. Limiting authorized access, including "hacking" and other unlawful activities; and
4. Limiting unauthorized disclosure, use, and dissemination of personal identification information.

Student Permission

Each student must sign the District's Acceptable Use Policy as a condition for using the District's electronic network. Each student and his or her parent(s)/guardian(s) must sign the Parent Permission Form and User Agreement before being granted unsupervised use.

All users of the District's computers and means of Internet access shall maintain the confidentiality of student records. Reasonable measure to protect against

unreasonable access shall be taken before confidential student information is loaded on the network.

STUDENT AND STAFF ACCESS TO NETWORKED INFORMATION RESOURCES

The developments in telecommunications and other new technologies shift the ways that information may be accessed, communicated, and transferred by members of society. These changes may also alter instruction and student learning. In general CUSD #1 supports access by students and staff to rich information resources along with the development by staff of appropriate skills to analyze and evaluate such resources. In a free and democratic society, access to information is a fundamental right of citizenship. Franklin CUSD #1 is pleased to offer students and adults access to a computer network so they can share ideas, transmit information, and contact others. As we begin to connect to the global community, the use of these new tools and systems will bring new responsibilities as well as opportunities.

What is Available?

Access to the Internet will enable students and staff members to explore thousands of libraries, databases, museums, and other repositories of information and to exchange communication with other Internet users around the world. Families should be aware that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate, or potentially offensive. Thus, Franklin CUSD #1 will place filtering software on all computers. While the purposes of CUSD #1 are to use Internet resources for constructive educational goals, students may find ways to access other materials even when filtering is in place. We believe that the benefits to students from access to the Internet in the form of information resources and opportunities for collaboration exceed the disadvantages. Ultimately, however, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources and determining if these resources should be used at school.

What is Expected of Computer Users?

Students and adults are responsible for appropriate behavior on the school's computer network just as they are in a classroom or on a school playground. The network is provided for students to conduct research and communicate with others. Access to network services will be provided to students and staff members who agree to act in a considerate and responsible manner. Communications on the network are often public in nature. General school rules for behavior and communication apply. It is expected that users will comply with district standards and the specific rules set forth below. The use of the network is a privilege, not a right, and may be revoked if abused. The user is

personally responsible for his/her actions in accessing and utilizing the school's computer resources. Users are advised never to access, keep, or send anything that they would not want their parents, teachers, or principal to see. Independent student use of telecommunications and electronic resources will be permitted upon submission of permission forms and agreement forms by parents.

What are the Policies?

*All staff members and students are expected to follow these guidelines and policies

1. Network storage areas may be treated like school lockers. Network administrators may review communications to maintain system integrity, and this will insure that users are using the system responsibly.
2. Users are expected to store their records on floppy disks or at defined areas on the network.
3. E-mail and chat rooms may be used for educational purposes only with permission from the instructor.
4. The following are not permitted:
a. sending or displaying offensive messages or pictures
b. using obscene language
c. hacking into the network or into any computer or engaging in practices that threaten the network
d. disclosure of personal identification information
e. harassing, insulting or attacking others
f. accessing or using sites or e-mail that contain graphics or text that are obscene, child pornographic or generally harmful to minors
g. downloading or installing any commercial software, shareware, or freeware onto hard drives or network drives unless the user has written permission from the Network Administrator.
h. copying other people's work or intruding into other people's files
i. damaging computers, computer systems or computer networks
j. violating copyright laws
k. using others' passwords
l. trespassing in others' folders, work or files
m. intentionally wasting limited recourses (such as printer ink or network bandwidth)
n. employing the network for commercial purposes

A good rule to follow is never view, send or access materials which you would not want your teachers and parents to see. Should users encounter such material by accident, they should report it to their teacher immediately.

What are the Rules?

These are the guidelines to follow to prevent the loss of network and/or Internet privilege at Franklin CUSD #1:

1. Notify an adult immediately if, by accident, you encounter materials which violate the rules of appropriate use.
2. BE PREPARED to be held accountable for your actions and for the loss of privileges if these rules are violated.

What are the Sanctions?

1. Violations may result in a loss of access.
2. Additional disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior.
3. When applicable, law enforcement agencies may be involved.

I understand that individuals may be held liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for guidance of Internet use - setting and conveying standards for my daughter or son to follow when selecting, sharing, or exploring information and media. I have read the enclosed agreement about the appropriate use of computers, Internet, and e-mail at the school. (Questions should be directed to the principal for clarification).