reviewed and updated periodically. Violations of the acceptable use guidelines shall be subject to consequences including, but not limited to, discipline up to and including expulsion, loss of the System use privileges, and referral to law enforcement authorities or other legal action, if appropriate.

GUIDELINES FOR ACCEPTABLE USE OF SCHOOL TECHNOLOGY SYSTEM BY STUDENTS

Acceptable Use

All student users of the School Technology System (System) must comply with the School Acceptable Use Guidelines and each school's Student Use Agreement.

The System shall include all computer hardware and software owned or operated by the school, the school electronic mail, the school web site and the school on-line services, bulletin board systems and other forms of direct electronic communications. "Use" of the System shall include use of or obtaining access to the System from any computer terminal whether owned or operated by the school. At ICRE-R, students may be permitted to use their personal computers in approved and supervised situations. Some acceptable activities include, but are not limited, the following: e-mailing friends and family, exploring; housing resources in local and distant communities, making program related purchases, registering for college course, training and/or workshops, exploring community resources for leisure, support, therapy, education, etc., exploring and or updating entitlement information, investigating medical information, exploring assistive technology resources, performing on-line banking activities.

Students have no expectation of privacy in their use of the System. The school has the right to access, review, copy, delete or disclose, as allowed by law, any message sent, received, or stored on the school's electronic mail system. The school has the rights to and does monitor use of the System by students, including students' access of the Internet, as part of System maintenance and to determine whether the use is consistent with federal and state laws and school policies and guidelines.

Each school has a "Student Use Agreement" form that must be signed by both the student and the parent/guardian yearly in order for the student to access the network, e-mail and the Internet independently. In addition, the student must annually initial the second page of the form that lists unacceptable use and consequences. Should a parent/guardian prefer that a student not have e-mail and Internet access, use of the computer is still possible for more "traditional" purposes such as word processing or teacher-directed Internet research.

Privileges

Access to the System is provided as a privilege by the school and may be revoked at any time. Inappropriate use may result in discipline up to and including expulsion and loss of System use privileges.

The System, including all information and documentation contained therein, is the property of the school except as otherwise provided by law.

Unacceptable Use

System uses listed below are prohibited and may result in discipline up to and including expulsion or other consequences as provided in the "Consequences for Violations" section of these Guidelines and each school's Behavioral Interventions Guidelines (BIG) and rules.

Computers, Internet, e-mail or other technology shall not be used for unacceptable purposes, including the following:

1. Disruption of the educational process or interference with the rights of others at any time, either during school hours or non-school hours.
2. Use of the System during any time period considered unacceptable by the school.
3. Use of inappropriate language or profanity.
4. Accessing or joining any on-line communication or social networking sites without specific prior written approval. (Including accessing social networking like Facebook, MySpace, Twitter, message boards, live journal or blog sites. Accessing chat rooms or accessing any instant message formats, e.g., AIM, AOL, ICQ. Joining listservs, newsgroups, or other automated newsletters such as Joke of the Day. Signing up for or logging into any account (like eBay) other than a DHS account without specific prior written approval. Entering any credit card numbers or purchasing anything through the Internet and/or e-mail.)
5. Accessing Internet-based e-mail (e.g. Hotmail, T-Mobile) other than the DHS e-mail system.
6. Accessing, retrieving, viewing or disseminating any material in violation of any federal or state laws or regulation or school policy or rules. This includes, but is not limited to, improper use of copyrighted material; improper use of the System to commit fraud or with the intent to commit fraud,; improper use of passwords or access codes; or disclosing the full name, home address or phone number of any student, school employee or system user.
7. Engaging in activities which are not related to school educational purposes or which are contrary to the instructions from supervising school employees as to the system's use.
8. Engaging in for-profit or non-school sponsored commercial activities, including advertising or sales.
9. Accessing, retrieving or viewing inappropriate matter using the school's network or any other network. Inappropriate matter includes: abusive, threatening, racially offensive, obscene, profane or indecent materials. "Indecent materials" are those materials which in context, depicts or describes sexual activities or organs in terms patently offensive, as measured by contemporary community standards. "Obscene materials" are those materials which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way in which, taken as a whole, do not have any serious literary, artistic, political or scientific value.
10. Accessing through the Internet and/or e-mail dating services, personal ads, adult-only or pornographic sites.

11. Sending electronic mail that is meant to harass, threaten, intimidate or demean an individual or group of individuals because of sex, color, race, religion, disability, national origin or sexual orientation including: nuisance electronic mail or other online messages; chain letters, pyramid schemes, or other unwelcome messages; and/or messages which include inappropriate language or profanity.
12. Sending mass electronic mail to multiple users without prior authorization by the superintendent or designee including using the Internet and/or e-mail for any illegal activity, product advertisement or political lobbying.
13. Gaining unauthorized access to or vandalizing the account, data or files of another including: using or tampering with another person's account or password; sharing your password with another person; disclosing another person's password; forging or improperly altering electronic mail messages.
14. Invading the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student records.
15. Downloading, copying, printing or otherwise storing or possessing any data which violates federal or state copyright laws or these guidelines.
16. Posting material on the school's web site without the authorization of the superintendent or designee.
17. Bypassing or attempting to bypass computer or computer-related security systems including tampering with anti-virus or Internet filtering software.
18. Attempting to transfer or transferring any software to or from the System without authorization from the System administrator. Includes, but is not limited to, programs, videos, video trainers, music files, photos, etc., whether or not it is copyrighted or free of viruses.
19. Attempting to gain or gaining unauthorized access to unauthorized programs, resources, or entities, including hacking or other unlawful online activities such as gambling or vandalizing the system or the technology system of any other individual or organization.
20. Disrupting or interfering with the system or tampering with or destroying computer equipment.
21. Bringing any type of personally owned or loaned software, hardware, computer-attachable media storage devices or media readers without specific parental written approval (ICRE-R and ISD only). Such equipment will be immediately confiscated and sent home at the student's expense, with disciplinary consequences commensurate with the infraction to be duly enforced.

Education, Supervision and Monitoring of Online Activities

Designated school personnel periodically monitor and review the access logs generated by the school's filtering system which includes Internet and e-mail usage. The Internet filtering system blocks visual depiction of:

1. Obscenity
2. Child pornography
3. Materials harmful to minors

Designated school personnel provide age-appropriate training for students who use the school's Internet facilities. The training provided is designed to promote the school's commitment to:

1. The standards and acceptable use of Internet services as set forth in the school's Internet Safety Policy.
2. Student safety with regard to:
    a. safety on the Internet;
    b. appropriate behavior while on online, on social networking Web sites and in chat rooms; and
    c. cyberbullying awareness and response.

Any violation to the school's Internet Safety Policy, Guidelines and Student Use Agreement are reported to appropriate staff including the school superintendent.

School, educational staff and lab monitors are instructed to continuously educate and 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. Staff 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 of other students or staff. Staff 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.

Off-site Use of Electronic Technology

The off-site use of electronic technology which disrupts or can reasonably be expected to disrupt the school environment will result in discipline up to and including expulsion.

The school may discipline a student whose personal web site or other off-site activity involving electronic technology causes, or can reasonably be expected to cause, a or disruption involved use of the school System.

Web Sites

Unless otherwise allowed by law, school web sites shall not display information about or photographs or works of students without written parental permission.

Any web site created by a student using the System must be part of a school sponsored activity or otherwise be authorized by the appropriate school administrator. All content, including links, or any web site created by a student using the System must receive prior approval by the classroom teacher or an appropriate school administrator. All contents of a web site created by a student using the System must conform to the tenets of the Acceptable Use Guidelines.

Disclaimer

The school makes no warranties of any kind, whether express or implied, for the System. The school is not responsible for any damages incurred, including the loss of data resulting from delays, non-deliveries, or service interruptions. Use of any information obtained via the System is at the user's own risk. The school is not responsible for the accuracy or quality of information obtained through the System. The school is not responsible for any user's intentional or unintentional access of material on the Internet which may be obscene, indecent or of an inappropriate nature.

Security and User Reporting Duties

Security in the System is a high priority and must be a priority for all users. Students are prohibited from sharing their log-in passwords with any other individuals. Any attempt to log in as another user will result in discipline up and including expulsion.

Vandalism

Vandalism or attempted vandalism to the System is prohibited and will result in discipline, which may include: (1) suspension or revocation of the System privileges, (2) other discipline including suspension or expulsion from school, and (3) referral to law enforcement authorities or other legal action in appropriate cases.

Consequences for Violations

A student who engages in any of the prohibited acts listed above may be subject to discipline up to and including expulsion. A student who believes that his/her System use privileges have been wrongfully limited may request a meeting with the building principal and school superintendent to review the limitation. The decision of the superintendent shall be final.

SECTION 5: STUDENT RECORDS POLICIES AND PROCEDURES

State and federal laws require that schools keep student school records confidential and allow parents/guardians to view, copy and correct records. The policy with regard to student records, including contents of permanent and temporary records, release of information, access to records and correction and modification of records has been developed to comply with the federal Family Educational Rights and Privacy Act (20 U.S.C. 1232g) and the regulations promulgated by the U.S. Department of Education (34 CFE Part 99), The Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.) and the Illinois School Student Records Act (105 ILCS 5) and the regulations promulgated by the Illinois State Board of Education (23 Ill. Adm. Code, Part 375).

CONSENT FOR DISCLOSURE OF RECORDS

The parent/guardian or eligible student may authorize the release of information to other persons by providing a signed and dated written consent which:

1. specifies the records that may be disclosed;
2. states the purpose of the disclosure; and