

GUIDELINES FOR ACCEPTABLE USE OF DISTRICT TECHNOLOGY SYSTEM BY EMPLOYEES

A. Acceptable Use

All users of the District Technology System must comply with the District's Acceptable Use Guidelines, as amended from time to time.

The System shall include all computer hardware and software owned or operated by the District, the District electronic mail, the District web site, and the District on-line services and bulletin board systems. Use of the System shall include use of or obtaining access to the System from any computer terminal whether owned or operated by the District.

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

Employees should be aware that their personal computer files or System use may be subject to public disclosure under the *Illinois Freedom of Information Act*.

Access to the System is provided to employees primarily for work-related purposes. Incidental personal use should be minimized.

B. Privileges

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

The System, including all information and documentation contained therein, is the property of the District, except as otherwise provided by law. The district technology coordinator periodically monitors and reviews the access logs generated by the filtering system (SonicWall Firewall and Internet Filter). This filtering system blocks the visual depiction of obscenity, child pornography, and materials harmful to minors.

C. Prohibited Use

Uses of the System listed below are prohibited and may result in discipline or other consequences provided in Section H of these Guidelines. The System shall **not** be used to:

1. Engage in activities which are inconsistent with the District's educational mission or which interfere with an employee's performance of work responsibilities.
2. Access, retrieve, or view obscene, profane or indecent materials. "Indecent materials" are those materials that, in context, depict or describe 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.
3. Access, retrieve, view or disseminate any material in violation of any federal or state laws or regulation or District 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, district employee, or user.
4. Transfer any software to or from the System without authorization from the System Administrator.
5. Engage in for-profit or non-school sponsored commercial activities, including advertising or sales.
6. Harass, threaten, intimidate, or demean an individual or group of individuals because of sex, color, race, religion, disability, national origin or sexual orientation.

7. Disrupt the educational process, including use that is reasonably foreseeable to result in a disruption, or interfere with the rights of others at any time, either during school days or after school hours.
8. Disrupt or interfere with the System.
9. Gain unauthorized access to or vandalize the data or files of another user.
10. Gain unauthorized access to or vandalize the System, or the technology system of any other individual or organization.
11. Forge or improperly alter electronic mail messages, use an account owned by another user without authorization, or disclose the user's individual password or that of another user.
12. Invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student records.
13. Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Guidelines.
14. Send nuisance electronic mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages.
15. Send mass electronic mail to multiple users without prior authorization by the appropriate District administrator.
16. Conceal or misrepresent the user's identity while using the System.
17. Post material on the District's web site without the authorization of the appropriate District administrator.

D. Web Sites

Unless otherwise allowed by law, the District web sites shall not display photographs or work of students without written parental permission.

Any web site created by an employee using the System must be part of a District-sponsored activity, or otherwise be authorized by the appropriate District administrator. All content, including links, of any web site created by an employee using the System must receive prior approval by the appropriate District administrator. All contents of a web site created by an employee using the System must conform with these Acceptable Use Guidelines. Employees may not place any personal or editorial material on the District web site or any web site created by an employee using the System.

E. Disclaimer

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

F. Security and User Reporting Duties

Security in the System is a high priority and must be a priority for all users.

Users are prohibited from sharing their login IDs or passwords with any other individual. Any attempt to log in as another user will result in consequences as set forth in Section H of these Guidelines.

A user who becomes aware of any security risk or misuse of the System must immediately notify the appropriate District administrator.

Employees are 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. Employees 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.

G. Vandalism

Vandalism or attempted vandalism to the System is prohibited and will result in consequences as set forth in Section H of these Guidelines. Vandalism includes, but is not limited to, the downloading, uploading, or creating computer viruses.

H. Consequences For Violations

Violations to the district's AUP/Internet Safety Policy are reported to the appropriate building principal. Any user of the System who engages in any of the prohibited acts listed above, shall be subject to discipline which may include: (1) discipline as provided in the District's policies, (2) suspension or revocation of System privileges, and (3) referral to law enforcement authorities or other legal action in appropriate cases.