

TECHNOLOGY USE & INTERNET SAFETY POLICY
Waterloo Community Unit School District No. 5
Updated April 1, 2007

The Board of Education hereby determines that it is in the best interests of the District, its personnel and its students, and members of the Waterloo Community Unit School District No. 5 community, to promote use of and familiarity with the District Technology System and with the services which are available through that System to support learning and enhance instruction, and to improve communications between the school and community.

Knowledgeable and appropriate use of the District Technology System can facilitate access to information resources available on-line, create innovative learning environments, and provide for worldwide communication. For purposes of this policy, implementing rules, and acceptable use guidelines, the term "District Technology System" or "System" shall include all computer hardware and software owned or operated by the District, District electronic mail, District web sites, and District on-line services and bulletin board systems. "Use" of the District Technology System shall include use of or obtaining access to the System from any computer terminal whether or not owned or operated by the District.

The District Technology System was established to comprise part of the school curriculum, and is intended by this Board to function in support of that curriculum and of students' mastery of the curriculum through improved communication between the school and students' parents or guardians. The District Technology System does not constitute a public forum. The District reserves and retains the right to regulate the content of and links to the District Technology System. The District also has the right to and does monitor use of its Technology System. Except as provided by federal and state statutes protecting the confidentiality of students' education records, no user of the District Technology System has an expectation of privacy in connection with such use.

The Board of Education recognizes that although the Internet and on-line services afford access to legitimate sources of information for academic and educational purposes, they also enable access to materials which may be illegal, obscene or indecent. The use of elements of the District Technology System including the Internet shall be consistent with the District's educational mission and the curriculum adopted by the Board.

With respect to any of its computers with Internet access, the District will use technology protection measures to (A) protect minors against access through such computers to visual depictions which are obscene, constitute child pornography, or are otherwise harmful to minors, and (B) protect all users against access through such computers to visual depictions that are obscene or constitute child pornography.

The Board of Education further recognizes that the effective operation of the District Technology System depends upon the existence and enforcement of guidelines for the efficient, ethical and legal use of its resources. The Administration is authorized to and shall adopt and enforce guidelines which limit the use of the System to educational purposes, and describe acceptable and ethical use of the System. The guidelines shall, among other points, address:

- A. access by minors to inappropriate matter on the Internet and World Wide Web;
- B. the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication;
- C. unauthorized access, including "hacking" and other unlawful activities by minors and other users online;
- D. unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
- E. measures designed to restrict minors' access to materials harmful to minors.

Such guidelines shall be distributed to District employees and students (and other members of the Waterloo Community School District No. 5 community) who are afforded access to the System.

Violation of the acceptable use guidelines shall be subject to consequences including but not limited to discipline, loss of System use privileges, and referral to law enforcement authorities or other legal action in appropriate cases.

**GUIDELINES FOR ACCEPTABLE USE OF
DISTRICT TECHNOLOGY SYSTEM BY EMPLOYEES
Updated April 1, 2007**

A. Acceptable Use

All users of the District Technology system ("System") must comply with the District 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 employees' access of the Internet, as part of System maintenance and 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 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.

C. Prohibited Use

The uses of the System listed below are prohibited and may result in discipline or other consequences as provided in section H of these guidelines. The System shall **not** be used to:

1. Engage in activities which are not related to District 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 which, 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 System user.
4. Transfer any software (programs) 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, District web sites shall not display information about or photographs or works 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 District administrator. All contents of a web site created by an employee using the System must conform to 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, misdeliveries, 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 which 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 log-in 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.

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, downloading, uploading, or creating computer viruses.

H. Consequences for Violations

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.

**AUTHORIZATION FOR ACCESS TO
DISTRICT TECHNOLOGY SYSTEM BY EMPLOYEES**

**This form must be read and signed by each user as a condition of using the
District Technology System.**

By signing this authorization, I acknowledge that I have received a copy of the "Guidelines for Acceptable Use of District Technology System by Employees" dated April 1, 2007, and that I have read, understand, and agree to follow the Guidelines.

I acknowledge that access to the District Technology system is provided as a privilege by the District and that inappropriate use may result in discipline.

I ACKNOWLEDGE THAT I HAVE NO EXPECTATION OF PRIVACY IN MY USE OF THE DISTRICT TECHNOLOGY SYSTEM AND THAT THE DISTRICT HAS THE RIGHT TO AND DOES MONITOR USE OF THE SYSTEM.

Name: _____

Signature: _____

Date: _____