Acceptable Use of District 24 Technology Network

For Students, Parents and Staff

All users of the District Technology Network ("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 website, and the District online services and access to the Internet. "Use" of the System shall include use of or obtaining access to the System from any computer whether owned or operated by the District.

Users have no expectation of privacy in their use of the System. The District (defined as the Superintendent and/or its designee) 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 users, including user's access to the Internet, as part of the System maintenance to determine whether the use is consistent with federal and state laws and District policies and guidelines.

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

The use of the District's network, including the Internet, is a privilege, not a right, and inappropriate use will result in a cancellation of this privilege. The System is to be used primarily for academic and administrative purposes and not as a public forum, or for general use.

Terms and Conditions

Acceptable/Appropriate Use – Access to the District's network including the Internet must be for the purpose of education or research and be consistent with the educational objectives of the District. Including, but not limited to:

1. Curricular and instructional activities or in support of such activities.
2. Research consistent with the goals and purposes of the District.
3. Communications between students, faculty, staff and the local and global communities.
4. Development and implementation of the curricula.
5. Professional development of staff members.
6. Administrative or managerial record-keeping, reporting data access or research.
7. Limited personal use by employees not to interfere with job responsibilities.

Unacceptable/Prohibited Use – Individuals are responsible for individual actions and activities involving the network.
Examples of unacceptable use include, but are not limited to:

1. Engage in activities which are inconsistent with the District's educational mission or which interferes 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 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 personal 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. Engage or participate in any activity against another person which constitutes "Cyber-Bullying" or "Cyber-Harassment".
8. 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.
9. Disrupt or interfere with the System.
10. Gain unauthorized access to or vandalize the data or files of another user.
11. Gain unauthorized access to or vandalize the System, or the technology system of any other individual or organization.
12. 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.
13. Invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student records.
14. Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Guidelines.
15. Send nuisance electronic mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages.
16. Send mass electronic mail to multiple users without prior authorization by the appropriate District administrator.
17. Conceal or misrepresent the user's identity while using the System.
18. Post material on the District's web site without the

authorization of the appropriate District administrator.
19. Wastefully using resources, such as file space.
20. Posting anonymous messages.
21. Using the network while access privileges are suspended or revoked.

E-mail Communications as Student Records — Employees must be aware that according to the Federal Family Educational Rights and Privacy Act and the Illinois School Student Records Act, electronic mail communications which "concern a student and by which a student may be individually identified", can qualify as the creation of a student record. Parents and/or students over age 18 exercising their statutory right to obtain access to their student files, by law, can be allowed access to this information. Employees should handle any email containing information about identifiable students in a confidential manner.

1. Care must be used in addressing such email communications, to ensure that they are sent only to authorized and intended recipients.
2. Distribution lists should be updated to keep addresses of intended recipients current, and to limit distribution only to people who are authorized to receive communication about particular students.

The Children's Internet Protection Act — Each District computer with Internet access shall have a filtering device that blocks entry to visual depictions that are:

1. Obscene.
2. Pornographic.
3. Harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the District.

The District shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purposes, provided the person receives prior permission from the District or system administrator. The District shall include measures to address the following:

1. Restricting student access to inappropriate matter and harmful materials.
2. Student safety and security when using electronic communication.
3. Limiting unauthorized access, including "hacking" and other unlawful activities.
4. Limiting unauthorized disclosure, use, and dissemination of personal identification information.

Network Etiquette – Individuals are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
1. Be polite. Do not become abusive in the messages to others.
2. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
3. Do not reveal personal address or telephone numbers of students or colleagues.
4. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities. All messages may be monitored or read by school officials.
5. Do not use the network in any way that would disrupt its use by other users.
6. All communications and information accessible via the network should be considered private property unless listed as public domain.

No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damage you suffer. This includes loss of or damage to data resulting from delays, non deliveries, missed deliveries, or service interruptions caused by its negligence, personal errors, or omissions. The District will not be responsible for any charges or fees resulting from unauthorized use of the Internet. Use of any information obtained via the network including the Internet is at your own risk. The District specifically denies any responsibilities for the accuracy or quality of information obtained through its services.

Indemnification - The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of any breach of procedures.

Security – Network security is a high priority. If an individual can identify a security problem on the network including the Internet, the individual must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep the individual account and password confidential. Do not use another individual's account without written permission from the individual or the classroom teacher. Attempts to log-on to the network including the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism – Vandalism will result in cancellation of privileges and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the network including the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.