DISTRICT ACCEPTABLE USE POLICY FOR EMPLOYEES

The Internet is an electronic highway connecting thousands of computers all over the world. O'Fallon School District No. 90 is pleased to have the technology and networks available to access the Internet, publish web pages and communicate using e-mail. Hardware is in place for users to access educational resources from anywhere in the world. With the technology now available, teachers and students can use computers to enhance lessons, prepare classroom materials, research topics, build academic skills and extend learning beyond the classroom.

Along with access to the Internet also comes the availability of material that may not be considered to be of educational value in the context of the school setting. The District Technology Use Policy restricts access to material that is inappropriate in the school environment and the School District has taken available precautions to restrict access to controversial materials through an Internet filtering program called Cyber Patrol. However, on a global network, it is impossible for filtering software to block every controversial and inappropriate site.

The District uses certain educationally appropriate online resources such as Google Apps for Education, BrainPop, Net Trekker, and Discovery Education to provide learning opportunities to our students. These online resources are reviewed and approved by the administration. The District may provide online vendors with a student's username, password, full name, and related information for the purpose of securing confidential credentials (i.e., username and password) and access for the student. This information will remain confidential and will not be shared except for the purpose of providing these services.

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.

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 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.

PURPOSE OF TECHNOLOGY

District technology, computers, and access to the Internet are designed for a limited educational purpose. The term "educational purpose" includes use of the network (hardware/software/connections, etc.) and access to the Internet for classroom activities, research, communications, career awareness, and professional development. Use of these educational tools is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges.

Employee use of technology, Internet, web publications and e-mail will be governed by the policies found in this document, related District regulations, employment policies and applicable collective bargaining agreements. 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.

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 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. All 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*.

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

Use of the technology, Internet, web publications and e-mail constitutes consent to abide by the policies contained in this document.

Use and access to the District's technology and related peripherals and software are not to be used for personnel, commercial, and political gain.

TECHNOLOGY AND COMPUTER USE

All employees shall assume the following responsibilities while using District technology and computers.

1. The District's networks, and its software, hardware, and data files, are owned and controlled by the School District. The District provides access to technology to staff members in fulfilling their duties and responsibilities, and as an educational tool. The District maintains the right to search all data contained on District computers and equipment.

2. Employees will treat all equipment with care and report any abuse or misuse as soon as they become aware of it to a teacher, a computer technician, or principal.

3. Employees will report any malfunction or problem as soon as they become aware of it to a computer technician, or principal.

4. Employees will not vandalize or otherwise **intentionally** damage any District technology hardware or software. If they do, they will be responsible to pay all repair and/or replacement costs. Vandalism is defined as any malicious attempt to harm or destroy data of another person, computer software, the network, computer hardware, computer wiring, or computer configuration.

5. Employees will not damage, destroy, or copy another person's data. If they do they will be referred Superintendent for disciplinary action.

6. Employees will not tamper with or attempt to gain access to computer data to which they have no security authorization. Doing so will result in the cancellation of privileges.

7. Employees will not load or copy unauthorized software onto District computers. All software used on District computers is to be properly licensed and registered with the publisher or manufacturer, and ***installed by District Technology personnel****.*

8. Employees who can identify a security problem on the District's network and/or Internet must notify a ***District Technology personnel*** or principal and should not demonstrate the problem to someone else.

9. Employees will not attempt to log-in to a computer or the District's network as a system administrator. Doing so will result in the cancellation of privileges.

10. Employees identified as a security risk may be denied access to the District's technology and computers.

11. Staff will not allow non-district employees (e.g., spouses, siblings, acquaintances, etc.) access to District's computers or network using their or anyone else's account information.

ACCESS

Full time District employees will be provided with an individual network and/or e-mail account in positions where it is needed in fulfilling their assigned duties and responsibilities and/or as an educational tool for use with students. Employees 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 disciplinary action. The Superintendent will make decisions regarding who will receive a District network and/or e-mail account.

INTERNET USE

The District's access to the Internet, and its software, hardware, and data files, are owned and controlled by the School District. The District provides Internet access to staff members in fulfilling their duties and responsibilities, and as an educational tool. The District maintains the right to monitor Internet use and maintain user logs. All users shall assume the following responsibilities while using the Internet.

Prohibited Uses - The uses of the System listed below are prohibited and may result in discipline or other consequences as provided in the "Due Process" section of these Guidelines, applicable Collective Bargaining Agreements, and the District's Board Policies. The System shall not be used to:

1. Engage in activities which are not related to District educational purposes or which are contrary to the instructions from supervising District employees as to the System's use.

2. Access, retrieve, or view obscene, hateful, 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 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 data, files, the System or the technology system of any other individual or organization.

10. Forge or improperly alter electronic mail messages, use an account owned by another user, or disclose the user's individual password or that of another user.

11. Invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student records.

12. Download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Guidelines.

13. Send nuisance electronic mail or other online messages such as chain letters, pyramid schemes, or obscene, harassing or other unwelcome messages.

14. Send mass electronic mail to multiple users without prior authorization by the appropriate District Administrator.

15. Conceal or misrepresent the user's identity while using the System.

16. Post material on the District's web site without the authorization of the appropriate District administrator.

17. Attempt to gain unauthorized access to the District network or use the District's network to access any other computer system. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".

18. Make deliberate attempts to disrupt computer performance or destroy data by any means including spreading computer viruses. These actions are illegal.

19. Use the District's networks to engage in any other illegal acts, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of another person, etc.

20. Use data created outside the school and brought in on mobile storage devices such as USB flash drives without scanning the data for viruses.

21. Use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

22. Engage in personal attacks, including prejudicial or discriminatory attacks, or knowingly or recklessly post false or defamatory information about a person or organization.

23. Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If an employee is told by a person to stop sending him/her messages, the employee must stop.

24. Post personal contact information or private information about themselves or other people. Personal contact information includes home address and telephone number and personal email address.

25. Utilize social networking sites and instant messaging to communicate with students, parents and other employees.

26. Repost a message that was sent to them privately without permission of the person who sent the message.

27. Plagiarize another person's work. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.

28. Infringe on another person's rights of copyright. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request written permission from the copyright owner.

29. Engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.

RESPECTING LIMITED RESOURCES

Employees will use the computers and networks only for educational activities and limited, high-quality, personal research.

WEB PAGE PUBLICATION

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 employees shall assume the following responsibilities while producing employee web pages that are created and posted for viewing outside the District's Intranet:

District/School Web Site/Pages: The District will establish a web site. Material appropriate for placement on the District web site includes: District information, school information, and teacher or class information. Personal, non-educationally-related information will not be allowed on the District web site. The District Technology Coordinator or his designee will be responsible for maintaining the District web site and monitoring all District web related activities.

Classroom Level Web Pages: Teachers may establish web pages for use with class activities or that provide a resource for other teachers or parents. Teachers will be responsible for maintaining their class or educational resource sites. For sites that require password-protected access, employees will ensure that passwords are only provided to the parents of students.

Web Page Publishing Guidelines:

Copyright Web Publishing Rules: Copyright law and District policy prohibit the republishing of text or graphics to the Web without explicit written permission by the original author.

- District web pages must not contain copyrighted or trademarked material belonging to others unless written permission to display such material has been obtained in writing from the owner.

- Staff and students engaged in producing web pages containing copyrighted material should provide the building principal or their designee with hard copy permissions before the web pages are published. Printed evidence of the status of "public domain" documents must be provided.

- The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide permission. If the material is web-based, the manager of the site may not be considered a source of permission.

- The "fair use" rules governing student printed reports (non web-based materials) in classrooms are less stringent and permit limited use of graphics and text. There will be no assumption that the publication of copyrighted material on a web site is within the fair use exemption.

Web Pages shall not:

1. Contain a student's full name. Only a student's **first name and last initial** can be displayed and must not be displayed without a signed release by parent or legal guardian.

2. Contain personal contact information about students beyond that permitted by the school (or district) and parent.

3. Display photographs or videos of any identifiable individual without a signed release by a parent or legal guardian.

4. Display a student's picture and name on the same page.

5. Contain copyrighted or trademarked material belonging to others unless written permission to display such material has been obtained from the owner. There will be no assumption that the publication of copyrighted material on a web site is within the fair use exemption.

6. Display photographs of students on a page that is not password-protected or otherwise available to the general public.

Web Pages shall:

1. Meet academic standards of proper spelling, grammar, and accuracy of information.

2. Be reviewed, updated, and maintained on a regular basis to insure the site is appropriate and has educational value. Active links must be tested for connectability and appropriateness.

3. Carry a stamp indicating when it was last updated and the e-mail address of the teacher responsible for the page.

4. Have a link that will help users find their way to the appropriate home page.

5. Be monitored and reviewed for timeliness. Once material is no longer germane to the particular lesson or educational mission, the employee shall remove it from the web page.

E-MAIL USE

- It will **not be** considered a violation of an employee's right to free speech to require removal of material that fails to meet established educational objectives or that is in violation of a provision of the Technology Use Policy or student disciplinary code.

- The District's electronic mail system, and its software, hardware, and data files, are owned and controlled by the School District. The District provides e-mail to staff members in fulfilling their duties and responsibilities, and as an educational tool. The District maintains the right to monitor e-mail use and maintain user logs. E-mail logs will not be maintained or backed-up for longer than thirty days. The Superintendent will make decisions regarding who will receive a District e-mail account.

- The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any staff member to an e-mail account is strictly prohibited.

- Each person should use the same degree of care in drafting an e-mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

- Electronic messages transmitted via the District's Internet gateway carry with them an identification of the user's Internet "domain." This domain name is a registered domain name and identifies the author as being with the School District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of the School District. Staff will be held personally responsible for the content of any and all electronic messages transmitted to external recipients.

- Any messages received from an unknown sender via the Internet should be deleted immediately. Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file being transmitted.

- Use of the School District's electronic mail system constitutes consent to these regulations.

Student use of email as part of a classroom activity:

Students may only use e-mail as part of a class activity. Students in grades K-8 may have a monitored and restricted individual account provided by the District. Individual accounts will only be accessible to teachers and students inside the District. On occasions individual student email accounts may be used to collaborate and communicate with students from other Districts in the United States or abroad. Material presented on a monitored restricted student account must meet the educational objectives of the class activity. Teachers will monitor student email use when they are participating in classroom activities requiring access to email. The District maintains the right to monitor e-mail use and maintain user logs. E-mail logs will not be maintained or backed-up for longer than thirty days. The Superintendent will make decisions regarding who will receive a District e-mail account.

DUE PROCESS

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through the District's network.

In the event there is an allegation that a user has violated the District Technology Use Policy, the person will be provided with a notice and opportunity to be heard in the manner set forth in the District regulations, policies and applicable collective bargaining agreements. Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the employee in gaining the self-discipline necessary to behave appropriately on an electronic network.

Any District administrator may request to terminate the account privileges of a staff member or guest user by providing notice to the user and the District Technology Coordinator. Staff member or guest accounts not active for more than 90 days may be removed, along with the user's files, without notice to the user.

SEARCH AND SEIZURE

Employees have a limited expectation of privacy with regard to the contents of their personal files, and online activity may be monitored while using the District's network.

Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the District Technology Use Policy. If this occurs, District regulations, employment policy, the collective bargaining agreement and/or the law will be used to resolve this situation.

An individual search will be conducted if there is reasonable suspicion that a user has violated the law or this Policy.

ACADEMIC FREEDOM, FREE SPEECH, AND SELECTION OF MATERIALS

Board policies on Academic Freedom and Free Speech will govern the use of the Internet.
When using the Internet for class activities, teachers will:

- Supervise their students when they are using the System.
- Not allow students to conduct random Internet searches in grades K-5. Students in grades K-5 should only go to teacher designated sites that have been previewed ahead of time and are related to the educational mission of the class. Teachers must supervise their students when they use the computer and access the Internet.
- Only allow students to conduct random searches in grades 6-8 on a limited basis to conduct research related to the educational mission of the class. Teachers must supervise their students when they use the computer and access the Internet.
- Select material that is appropriate in light of the age of the students and that is relevant to the educational objectives.
- Preview the materials and sites they require students to access to determine the appropriateness of the material contained on or accessed through the site.
- Provide guidelines and lists of resources to help students focus their research activities effectively and properly.
- Assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

WARRANTY

The School District makes no warranties of any kind, whether expressed or implied, for the service it is providing nor is it responsible for any damages suffered by a user. This includes loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by it's own negligence or the users errors or omissions. Use of any information is at the users own risk. The School District specifically denies any responsibility for the accuracy or quality of information obtained through its services. 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.

INDEMNIFICATION

The user agrees to indemnify the School District for any losses, cost, or damages, including reasonable attorney fees, incurred by the School District relating to, or arising out of, any breach of the authorization.

TELEPHONE CHARGES

The School District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line cost.