Instruction

Acceptable Use Policy for Use of District Technology

Acceptable Use

All users of the District Technology System ("System") must comply with the District's Acceptable Use Policy (AUP). "User" is defined as any individual who uses the System. These guidelines may change and notice will be given to stakeholders through www.jsd117.org. The Board's comprehensive policy manual is available for public inspection through the District's website www.jsd117.org or at the Board office located at: 516 Jordan St., Jacksonville, IL 62650.

A signed AUP must be on file for each User no later than 10 school days after the start of the school year. It is also understood that this document goes into effect beginning with the first day of school. The AUP is to be electronically acknowledged online during registration or upon entering as a new student to the district. Users with no AUP on file after the 10th day will be denied access to the System.

The System shall include:

- Personal devices when connected to the System
- All device hardware and software owned or operated by the District
- District electronic mail, website, and browser-based services (e.g. Skyward, District Google accounts)
- District affiliated social media services
- District wired and wireless network access

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

"Use" of the System shall include use of or obtaining access to the System from any device whether or not owned or operated by the District.

The Board of Education of Jacksonville School District 117 supports the use of the Internet and other computer networks in the District's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research, and collaboration. Use of the System shall be consistent with the curriculum adopted by the school district, as well as the varied instructional needs, learning styles, abilities, and developmental levels of users.

Authority

The electronic information available to users does not imply endorsement of the content by the school district, nor does the District guarantee the accuracy of information received on the Internet. The District shall not be responsible for any information that may be lost, damaged, or unavailable when using the System or for any information that is retrieved via the Internet. While the District takes precautions to restrict controversial material, it is impossible to restrict all materials that might be deemed controversial.

The school district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

Users 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 user files accessed through the System. The District has the right to and does monitor use of the System by users, including access of the Internet, as part of System maintenance and to determine whether use is consistent with federal and state laws and District policies and guidelines.

The Board establishes that use of the System is a privilege, not a right; inappropriate, unauthorized, and illegal use will result in the cancellation of those privileges and appropriate disciplinary action.

Responsibility

The District shall provide reasonable effort and supervision to ensure that this educational resource is used responsibly. Administrators, teachers, and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students are responsible for appropriate behavior on the District's System just as they are in a classroom or on a playground.

No warranty, expressed or implied, is made as to the quality or extent of Internet service or access by users on the District's system. The District shall not be responsible for any damages the user suffers. This includes, but is not limited to, damage to personal devices, loss of data from delays, non- deliveries, missed- deliveries, or service interruptions caused by negligence, errors, or omissions. Use of information obtained via the Internet is at the user's own risk. 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.

Network Guidelines

Network accounts will be used only by the authorized owner of the account for its authorized purpose. System users shall respect the privacy of other users on the system. Each user is responsible for his/her individual account and must take all reasonable precautions to prevent others from being able to use their account(s).

Prohibitions

Users are expected to act in a responsible, ethical, and legal manner in accordance with District policy, accepted rules of network etiquette, and federal and state law. Prohibitions include but are not limited to the following:

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, profane, or indecent materials, which, taken as a whole, do not have any literary, artistic, political, or scientific value that is connected to the District curriculum.
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 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. Use of the System for commercial or for-profit purposes.

6. Use of social networking of any form (e.g. Facebook, Twitter, Yahoo mail, Google for Education) unless approved by a District Administrator for educational purposes.
7. Use of the System for product advertisement for political lobbying.
8. Use of the System to harass, threaten, intimidate, or demean an individual or group of individuals for any reason including but not limited to: sex, color, race, religion, disability, national origin, or sexual orientation.
9. Use -of the System to 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.
10. Gain unauthorized access to or vandalize the data or files of another user.
11. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
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. Use of the System to invade the privacy of any individual, including violating federal or state laws regarding limitations on the disclosure of student records.
14. Use of the System to download, copy, print or otherwise store or possess any data which violates federal or state copyright laws or these Guidelines.
15. Use of the System to search for inappropriate sites/content. Internet searches are to be curricular related.
16. Use of the System to intentionally obtain or modify files, passwords, and data belonging to other users.
17. Conceal or misrepresent the user's identity, or the use of any means to remain anonymous while using the System.
18. Installation, loading, or use of unauthorized games, program files, or other electronic media.
19. Destruction, modification, or abuse of network hardware and software.
20. Using the System while access privileges are suspended or revoked.
21. Using another person's account or password.
22. Possessing personal storage devices that contain executable files including but not limited to portable browsers, hacking tools, network sniffers, etc. Personal storage devices may only be used to store non-executable files unless prior approval is granted by the system administrator.

<u>Consequences for Inappropriate Use</u>

1. The District may discipline a user whose personal web site or other off-site activity involving electronic technology causes, or can be reasonably be expected to cause, a substantial disruption of the school environment, without regard to whether that activity or disruption involved the use of the System.
2. The System user shall be responsible for damages to equipment, systems, and software resulting from deliberate or willful acts that violate this policy.
3. General standards of good behavior and communication apply when using the System. Any user of the System who engages in any of the prohibited acts listed above, shall be subject to discipline which may include:

   a. discipline as provided in the District's policies,
   b. suspension or revocation of System privileges, and
   c. referral to law enforcement authorities or other legal action in appropriate cases.

4. The building administrator shall have the authority to determine what constitutes inappropriate use, and his/her decision is final.

5. Illegal use of the System, intentional deletion or damage to files of data belonging to others, copyrighting violations, or theft of services will be reported to the appropriate legal authorities for possible prosecution.

6. Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any part of the System. This includes, but is not limited to, uploading or creation of computer viruses.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:

1. Users shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in with another user's name.

3. Users identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

4. If a user identifies a security problem, he/she must notify the appropriate building personnel. Building personnel will notify the District's system administrator. Do not demonstrate the problem to others.

5. Attempts to log on to the System as a system administrator by anyone other than the system administrator will result in cancellation of user privileges.

Safety

Reasonable and good faith efforts shall be employed to protect users from harassment or unwanted or unsolicited electronic communication. Any user who receives threatening or unwelcome communications shall immediately bring them to the attention of the appropriate building personnel. Building personnel will notify the appropriate building administrator. The building administrator will notify the district system administrator.

User shall not reveal personal addresses to other users on the network, unless required to do so by law or court order.

ADOPTED: June 21, 2017