

WOODSTOCK COMMUNITY UNIT SCHOOL DISTRICT 200

Authorization for Electronic Network Access

Expectations and Procedures

Please read this document carefully before signing the last page.

- *Students and their parents/guardians are expected to sign this Authorization for Electronic Network Access upon enrollment in grades 3, 6, and 9 or initial enrollment in the district.*
- *Staff members need only sign this Authorization for Electronic Network Access once while employed by the School District.*
- *Other approved users need to sign this Authorization for Electronic Network Access at the start of each activity approved by the district.*

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

TERMS AND CONDITIONS

Authorized User – Students, teachers, administrators, other employees of the District, and Board of Education, and other individual specifically authorized by the Superintendent or Designee shall be allowed access to the District computer network consistent with the District's curriculum, educational mission and this Policy and its implementing Administrative Procedures.

Acceptable Use - Access to the District's electronic network must be: (a) for the purpose of education or research, and be consistent with the District's educational objectives, or (b) for legitimate business use.

Privileges - The use of the District's electronic network is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator, in collaboration with district and/or building administrators, will make all decisions regarding whether or not a user has violated these procedures and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use - The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

- a. Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any State or federal law;
- b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
- c. Downloading copyrighted material for other than personal use;
- d. Using the network for private financial or commercial gain;
- e. Wastefully using resources, such as file space;
- f. Hacking or gaining unauthorized access to files, resources, or entities;
- g. Invading the privacy of individuals, that includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature including a photograph;
- h. Using another user's account or password;
- i. Posting material authored or created by another without his/her consent;
- j. Posting anonymous messages;
- k. Using the network for commercial or private advertising;
- l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
- m. Using the network while access privileges are suspended or revoked.
- n. Using the network in any way that would disrupt its use by other users.

Online Etiquette - The user is expected to abide by the generally accepted rules of online etiquette. These include, but are not limited to, the following:

- a. Be polite. Do not become abusive in messages to others.

- b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
- c. Do not reveal personal information, including the addresses or telephone numbers, of students or colleagues.
- d. Recognize that all electronic mail (e-mail) is not private. People who operate the system (Gmail, Yahoo Mail, etc.) have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities. Mail created on the district's Groupwise system may be accessible to members of the public through the Freedom of Information Act. Caution and care is to be used when sending any type of electronic mail through any system.
- e. Do not use the network or online systems in any way that would disrupt its use by other users.
- f. Consider all communications and information accessible via the network to be the property of the individual who created it. Appropriate copyright laws should be followed when using material accessed online or through electronic media.
- g. Report any suspicious activity, messages, or information to your supervisor or building administrator.
- h. Social networking sites should be used with the same considerations described above. District staff members are encouraged to limit their use of these types of electronic communications with students to those topics that directly relate to their positions in the district. While it is acceptable to e-mail student's homework and school related information, it is unadvisable to engage in personal conversations with students via electronic social media.
- i. Refer to district website for additional resources on internet safety tips and practices.

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 damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

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

Security - Network security is a high priority. If the user can identify a security problem on the Internet, the user must notify the system administrator or Building Principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. Attempts to log-on to 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/Theft - Vandalism or theft of any type of technology equipment or software 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 Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses. Restitution and police involvement may be required in instances of theft or vandalism.

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

Copyright Web Publishing Rules - Copyright law and District policy prohibit the re-publishing of text or graphics found on the Web or on District Web sites or file servers without explicit written permission.

- a. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
- b. Students and staff engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.
- c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission.
- d. The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- e. Student work may only be published if there is written permission from both the parent/guardian and student.

Privacy - Users shall have no expectation of privacy regarding files stored on school-based computers, servers, or other school-based electronic devices (i.e. district purchased cell phones, iPads, Kindle's, etc). Electronic files, including but not limited to e-mail, web pages, photos, and electronic books, stored on any district electronic media or stored outside of school using the district's Internet account are deemed to be property of the district. The System Administrator and

designee appointed by the superintendent may review files and messages to maintain system integrity and insure that users are acting responsibly.

Use of Electronic Mail - The District's electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the School District. The School District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.

- a. 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 student or staff member to an electronic mail account is strictly prohibited.
- b. Each person should use the same degree of care in drafting an electronic 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.
- c. Electronic messages transmitted via the School 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. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.
- d. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. 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 so transmitted.
- e. Use of the School District's electronic mail system constitutes consent to these regulations.

Social Networking – These sites should be used with caution and appropriate discretion. Information that is posted on these sites remains on the sites for an indefinite period of time. While there are certainly appropriate educational uses for social networking sites, district staff members are encouraged to limit their use of the social networking sites to those topics that directly relate to the educational needs of the students. It is acceptable to e-mail or post student homework assignments, information about curriculum topic covered in a specific course, and school related information. It is **unadvisable** for any staff member to engage in personal conversations or postings with students via electronic social media.

INTERNET SAFETY

Internet access is limited to only those "acceptable uses" as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in these procedures, and otherwise follow these procedures.

Staff members shall supervise students while students are using District Internet access to ensure that the students abide by the Terms and Conditions for Internet access contained in these procedures.

Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.

The system administrator and Building Principals shall monitor student Internet access.

Authorization for Electronic Network Access Form

Students and their parents/guardians are expected to sign this Authorization for Electronic Network Access upon enrollment in grades 3, 6, and 9 or initial enrollment in the district.

Staff members need only sign this Authorization for Electronic Network Access once while employed by the School District.

Other approved users need to sign this Authorization for Electronic Network Access at the start of each activity approved by the district.

- Please check the appropriate box: Staff Member
 Parent/Guardian of Student
 Student *
 Other Authorized User

I understand and will abide by the above *Authorization for Electronic Network Access*. I understand that the District and/or its agents may access and monitor my use of the Internet, including my e-mail and downloaded material, without prior notice to me. I further understand that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's electronic network connection and having access to public networks, I hereby release the School District and its School Board members, employees, and agents from any claims and damages arising from my use of, or inability to use the Internet.

User Name (*please print*)

User Signature

Date

*** Students are required to have a parent/guardian read and agree to the following:**

I have read this *Authorization for Electronic Network Access*. I understand that access is designed for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the network. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the terms of this *Authorization* with my child. I hereby request that my child be allowed access to the District's Internet.

Parent/Guardian Name (*please print*)

Parent/Guardian Signature

Date

Please detach this form and return it to your building principal, supervisor, or district office. The Authorization for Network Access Expectations and Procedures document is for your records.