

User Name _____
(please print)

**Kaneland CUSD #302 - Acceptable Use Policy
Authorization for Network Access**

Any person (i.e., full-time and part-time employees, students, substitute or student teachers, Board members, volunteers, citizens) using the district's network, shall use this resource only for school- and education-related purposes consistent with the goals of Kaneland CUSD 302. These include but are not limited to facilitating teaching and learning through resource sharing, innovation, and communication. Accessing the network through the District's computer system is a privilege that is granted, revoked or restricted at the discretion of the Board of Education through the administration. Misuse of the District's network access through, for example, unacceptable uses, violation of network etiquette, safety or security, vandalism or copyright infringement, may result in revocation or restriction of access to this resource. Specific terms and conditions for accessing the District's network are available in the administrative procedures, which are attached to this document and can be obtained in the main office at any Kaneland School. All users must sign this form indicating they agree and will abide to the terms and conditions contained within the administrative procedures.

Kaneland Student, Employee or Other Network User:

I understand and will abide by the above Authorization for Network Access. 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 network and having access to public resources, I hereby release the School District and its Board members, employees, and agents from any claims and damages arising from my use, or inability to use the District network or Internet.

USER SIGNATURE: _____ DATE: _____

(Required if the user is a student):

I have read this Authorization for 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 network or Internet.

PARENT/GUARDIAN NAME: _____
(Please print)

STUDENT NAME: _____
(Please print)

PARENT/GUARDIAN SIGNATURE: _____

DATE: _____

KANELAND COMMUNITY UNIT SCHOOL DISTRICT #302
Administrative Procedures for Access to the District Network (Internet Safety Policy)

All Kaneland employees and students (and their parents or guardians) must sign the Authorization for Network Access as a condition for using the District's Network and Internet connection. School Board members, administrators, community members and parents are treated like employees for the purposes of the Authorization. Please read this document carefully before signing the Authorization for Network Access form.

All use of the District's Internet access shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This Authorization does not attempt to state all allowed, required or proscribed behaviors by users. However, some specific examples are provided. The failure of any user to follow the terms of the Authorization for Network Access may result in the loss of privileges, disciplinary action, and/or appropriate legal action. The signatures on the Authorization for Network Access form are legally binding and indicate the signers have read the terms and conditions carefully and understand their significance.

Terms and Conditions

1. **Acceptable Use** –The District's Internet access must be used for the purpose of education or school-related research, and be consistent with the educational objectives of the District.
2. **Privilege of Use** – Using the District's Internet access is a privilege, not a right, and inappropriate use may result in cancellation of those privileges. The system administrator and/or school principal will make all decisions regarding whether or not a user has violated this Authorization and may deny, revoke, restrict or suspend access at any time.
3. **Unacceptable Use** – You are responsible for your actions and activities involving the network. Some examples of unacceptable uses are:
 - a. Using the network for any illegal activity, including "hacking", violation of copyright or other contracts, or transmission of any material in violation of any U.S. or State regulation;
 - b. Unauthorized downloading or loading of software;
 - c. Using unauthorized copyrighted materials or any other materials in violation of state, federal or international copyright laws;
 - d. Using the network for private financial or commercial gain, including advertising;
 - e. Wastefully using resources, such as network bandwidth and/or storage space;
 - f. Using of any unauthorized personal equipment attached, connected, and/or installed to district network;
 - g. Invading the privacy of individuals by unauthorized disclosure, use or dissemination of personal information;
 - h. Using another user's account or password;
 - i. Posting material authored or created by another without his/her consent, including anonymous messages;
 - j. Using the network to obtain, solicit or distribute information that could potentially incite illegal activity including violence, harassment, stalking or terrorist activity;
 - k. Using profanity, obscenity or language that is possibly considered offensive or threatening to persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities;
 - l. Using the network while access privileges are suspended or revoked;
 - m. Tampering with any electronic records, software, or equipment; and
 - n. Gaining any form of unauthorized access to resources or entities, as stated above or otherwise.
4. **Network Etiquette** – You are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:
 - a. Be polite. Do not become abusive in your messages to others.
 - b. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
 - c. Keep personal information, including the logins, passwords, addresses, and telephone numbers of students or colleagues confidential.
 - d. Recognize that electronic mail (e-mail) is not private. People who operate this system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
 - e. Use these resources so as not to disrupt service to other authorized users.
 - f. Consider all communications and information accessible via the network to be private property.
5. **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 you suffer. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or your errors or omissions. Use of any information obtained

via the Internet is at your own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

6. Indemnification – The user agrees to indemnify the School District for any loss, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this Authorization.
7. Internet Safety – Pursuant to the Children's Internet Protection Act, Kaneland uses filtering software to screen Internet sites for offensive material. Users are cautioned that many internet sites contain offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: Adult Content; Nudity; Sex; Gambling; Violence; Weapons; Hacking; Personals /Dating; Lingerie/Swimsuit; Racism/Hate; Tasteless; and Illegal/Questionable. In general it is difficult to eliminate all contact with this type of material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Authorized users accessing the Internet do so at their own risk. No filtering software is one hundred percent effective and it is possible that the software could fail. In the event that the filtering software is unsuccessful and children and staff gain access to inappropriate and/or harmful material, the Board will not be liable. To minimize these risks, use of the Kaneland Network is governed by this policy.
8. Vandalism – All authorized student users are to report promptly any violations of this policy to their teacher or school principal. The teacher or school principal will report such violations to the Technology Director or designee of the Kaneland Public Schools in order to ensure network security.

In order to maintain the security of the Kaneland System, authorized users are prohibited from engaging in the following actions:

- a. Intentionally disrupting the use of the Kaneland Network for other users, including, but not limited to, disruptive use of any processes or programs, sharing logins and passwords or utilizing tools for ascertaining passwords, spreading computer viruses, engaging in "hacking" of any kind, use of proxy or filter avoidance software or devices, and/or engaging in computer tampering of any kind.
 - b. Violating standard security procedures. Network security is a high priority. If you can identify a security problem on the network, you must notify a system administrator. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account. Attempts to log on to the network as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.
9. Copyright Web Publishing Rules – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Web sites or file servers without explicit written permission.
 - a. For each republication (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 sources.
 - b. Students and staff engaged in producing web pages must acquire and retain proof of the appropriate bibliographic references and permissions and, upon the district's request, provide the school district with documentation of these references and permissions. Printed evidence of the "public domain" status of documents must also be retained and provided to the district by students or staff if requested.
 - 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 on the Internet if there is written permission from both the parent/guardian and student.
 10. Use of Electronic Communication
 - a. The District's electronic communication systems, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides electronic resources to aid students and staff members in fulfilling their duties and responsibilities, and as an education tool.
 - b. 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 electronic resources (e.g., e-mail, chat rooms, and other unauthorized electronic communications) is strictly prohibited.
 - c. Each person should use the same degree of care in drafting an electronic message as would be put into a written memorandum or document. Users will be held personally responsible for their content of any and all electronic messages.