

Appendix VII

EMPLOYEE ONLINE ACCEPTABLE USE CONSENT FORM

I understand and will abide by the Park Rapids Area School District 309 Acceptable Use Policy. All use of the District 309's computers and Internet shall be consistent with District 309's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. This Authorization does not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. The failure of any user to follow the terms of the Authorization for Computer use, Local Area Network use and Internet Access will result in the loss of privileges, disciplinary action, and/or appropriate legal action. The signature(s) at the end of this document is legally binding and indicates the party who signed has read the terms and conditions carefully and understands their significance.

All computer use can be monitored, including e-mail, to see that the accounts are being used for the stated purposes. For this and other reasons, e-mail is not private. The district also uses remote management and remote viewing tools, with the ability to remotely take control and view any workstation on the network. Information Technology (IT) can use remote management and viewing at any time, and may at times inconvenience users. We will do our utmost to minimize disruptions.

By signing this authorization, users understand they allow remote access and remote viewing and will not disconnect any Information Technology technician from your workstation at any time.

Access to District 309's Network and Internet must be for the purpose of education or research, and be consistent with the educational objectives of District 309.

Privileges: The use of District 309's computers and Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The Director of Information Technology, and/or the building principal and School Administration will make all decisions regarding whether or not a user has violated this Authorization and may deny, revoke, or suspend access at any time. His or her decision is final.

Unacceptable Use: You are responsible for your actions and activities involving Internet use and the network.

- a. Using the network for any illegal activity, including violation of copyright or other contracts, sending threatening messages, engaging in child pornography or transmitting any material in violation of any U.S. or State regulation;
- b. Unauthorized downloading or copying software;
- 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. Gaining unauthorized access to resources or entities;
- g. Invading the privacy of individuals;
- h. Using another user's account or password;
- i. Posting material authored or created by another without his/her consent;
- j. Chatting (live-time communication)
- k. Viewing, downloading or printing obscene or inappropriate materials
- l. Failing to report known violations
- m. Using Novell instant messenger, send or broadcast any message on the Local Area Network or Wide Area Network
- n. Using the network for commercial or private advertising;
- o. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
- p. Using the network while access privileges are suspended or revoked.

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. Do not reveal the personal addresses or telephone numbers of students or colleagues;
- d. 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;
- e. Do not use the network in any way that would disrupt its use by other users.
- f. Consider all communications and information accessible via the network to be private property.

No Warranties: District 309 makes no warranties of any kind, whether expressed or implied, for the service it is providing. District 309 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. District 309 specifically denies any responsibility for the accuracy or quality of information obtained through its service.

Equipment: In order to encourage the integration of technology into curriculum and promote the acquisition and maintenance of technology skills, the Park Rapids Area Schools allows employees to use district computer technology off of District 309 property. This may include the use of district-owned personal computers, tablets, printers, and other devices. The equipment being used at a personal residence must not be used in any manner that will violate any local, state or federal law or the district policy.

Legal ownership of the equipment remains with the District. Employees will return the technology equipment and accessories at the time of termination of employment. The District reserves the right to repossess equipment and accessories at any time. The District may also choose to limit and/or withdraw home use privileges for failure to comply. Failure to return the property in a timely fashion may result in the involvement of law enforcement.

Indemnification: The user agrees to indemnify District 309 for any losses, costs, or damages, including reasonable attorney fees, incurred by District 309 relating to, or arising out of, any breach of the Authorization.

Security: Network security is a high priority. If you can identify a security problem on the Internet, you must notify the system administrator or the Director of Information Technology. 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 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 Internet, or any other network. This includes, but is not limited to, the uploading, downloading or creation of computer viruses.

Employee

By signing below, I agree to follow Park Rapids Area Schools' Electronic Technologies Acceptable Use policy. I understand that my use of the network is a privilege and requires proper online etiquette. I further understand that misuse of the network will result in disciplinary action.

Employee Name (PRINT) _____

Employee's Signature _____

School Building _____

Date _____

Return this form to the District Office.