Laura Ingalls Wilder Elementary
Christine Stefani - Principal
22130 NE 133rd Street • Woodinville, WA 98077
Office: (425) 936-2740 • Fax: (425) 702-0114

IMPORTANT: PLEASE SIGN AND RETURN

Dear Wilder Parents and Students,

Attached is Lake Washington School District's Acceptable Use Policy. Acknowledgment of this Policy is required before the use of school computers. Please review this policy with your child, sign, date, and return to school as soon as possible. These policies can also on the Lake Washington School District website. The links are: https://www.lwsd.org/about-us/policy-and-regulations/instruction-2000/electronic-resources-and-internet-safety-2022

https://www.lwsd.org/about-us/policy-and-regulations/instruction-2000/electronic-resources-and-internet-safety-2022

Thank you for your cooperation.

Ms. Stefani
Principal, Wilder Elementary

_____ _____

PRINT NAME (STUDENT) SIGNATURE (STUDENT)

_____ _____

PRINT NAME (PARENT) SIGNATURE (PARENT)

_____

DATE

Student Laptop Acceptable Use Procedures

Scope

The following procedures apply to all District students and cover all aspects of the District network. The district network includes wired and wireless computers/devices and peripheral equipment, files and storage, e-mail, and Internet content and all computer software, applications, or resources licensed to the District.

Appropriate Network Use

The District expects students to exercise good judgment and use the computer equipment in an appropriate manner. Use of the equipment is expected to be related to educational purposes.

Should personal equipment be used on the district's networks, the district reserves the right to gain access to the device for analysis to resolve any identified issues or threats. As a condition of using the district's networks, a student will provide requested device immediately.

Unacceptable/Prohibited network use by students includes:

- Commercial Use: Using District Network for personal or private gain, personal business, or commercial advantage is prohibited.
- Political Use: Using District Network for political purposes in violation of federal, state, or local laws is prohibited. This prohibition includes using District computers to assist or to advocate, directly or indirectly, for or against a ballot proposition and/or the election of any person to any office.
- Illegal or Indecent Use: Using District Network for illegal, bullying, harassing, vandalizing, inappropriate, or indecent purposes (including accessing, storing, or viewing pornographic, indecent, or otherwise inappropriate material), or in support of such activities is prohibited. Illegal activities are any violations of federal, state, or local laws (for example, copyright infringement, publishing defamatory information, or committing fraud). Harassment includes slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, pranks, or verbal conduct relating to an individual that (1) have the purpose or effect or creating an intimidating, a hostile. or offensive environment; (2) have the purpose or effect of unreasonably interfering with an individual's work or school performance, or (3) interfere with school operations. Vandalism is any attempt to harm or destroy the operating system, application software, or data. Inappropriate use includes any violation of the purpose and goal of the network. Indecent activities include violations of generally accepted social standards for use of publicly-owned and operated equipment.
- Disruptive Use: District network may not be used to interfere or disrupt other users, services, or equipment. For example, disruptions include distribution of unsolicited advertising ("Spam"), propagation of computer viruses, distribution of large quantities of information that may overwhelm the system (chain letters, network games, or broadcasting messages), and any unauthorized access to or destruction of District computers or other resources accessible through the District's computer network ("Cracking" or "Hacking").
- Personal Use: District Network may not be used for purposes of personal use not specifically authorized by a teacher or other district staff member. This includes connecting personal devices to the district network.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's computer network or the Internet.

Internet Safety

Students should not reveal personal information, including home address and phone number on web sites, e-mail, or as content on any other electronic medium. Students should not reveal personal information about another individual on any electronic medium. No student pictures or

names can be published on any class, school, or district web site unless the appropriate permission has been verified according to district policy. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Internet Safety Instruction

All students will be educated about cyber bullying awareness and response and about appropriate online behavior, including interacting with other individuals on email and/or on social networking sites and in chat rooms. Schools will make every effort to provide Internet Safety Instruction; however, in the absence of such instruction, students are still expected to follow all Acceptable Use Procedures (AUP). Age appropriate training materials will be made available to administration, staff, and families.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered as identified by the superintendent or designee.

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to district browser settings, use of personal portable Wi-Fi devices, and any other techniques designed to evade filtering or enable the publication of inappropriate content;
- The use of USB (aka thumb drive) emulators to run games, bypass proxy, or otherwise run non-district installed .exe files or other emulation software is strictly prohibited. USB drives should only be used for non-executable, school related content;
- District provided storage (e.g., One Drive, portal, Outlook, laptop hard drive, PowerSchool Learning, or Class Notebook) is for storing only content generated as part of the student's education or required for educational process. Attempt to store or storage of games or any executable files or inappropriate content is strictly prohibited;
- E-mail inconsistent with the educational mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
- The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers;
- Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively.

Network Security and Privacy

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account, for authorized district purposes. Students are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- Do not use another user's account;
- Do not use personal wireless hotspot devices;
- Do not connect personal smartphones, personal computers, personal storage devices, or any non-district device to the district's network;
- Do not insert passwords into e-mail or other communications;

- If you write down your account password, keep it out of sight;
- Do not store passwords in a file without encryption;
- Do not use the “remember password” feature of Internet browsers; and
- Lock the screen or log-off if leaving the computer.

Attempts to install or installation of malware, proxy bypass software, network, administration tools, local administration tools, or any software, malware, or tool that allows for the manipulation of user accounts or administrative privileges are strictly prohibited. Such install attempts or installation of such malware, software, or tools will be considered exceptional misconduct.

Student Data

District staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA). Permission to publish any student work requires permission from the parent or guardian.

Privacy

The District network, computers, internet, and use of e mail are not inherently secure or private. The district reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and,
- Any and all information transmitted or received in connection with network and e-mail use.

The district reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Copyright

Downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Discipline

Violation of any of the conditions of use explained in the Student Use of Electronic Resources policy or in these Acceptable Use Procedures (AUP) could be cause for disciplinary action, up to and including revocation of network and computer access privileges, restitution, suspension or expulsion, and/or police report in accordance with District Student Discipline Policies and Procedures.