Lake Washington School District

Book	Administrative Policies
Section	Section 2000 - Instruction
Title	Procedure Electronic Resources And Internet Safety
Code	2022P
Status	Active
Adopted	September 1, 2019

Student 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 otherl 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.

Staff Acceptable Use Procedures (AUP)

Scope

The following procedures apply to all district staff 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 staff to exercise good judgment and use the computer equipment in an appropriate and professional manner. Use of the equipment is expected to be related to the District's goals of educating students and/or conducting District business. The District recognizes, however, that some personal use is inevitable, and that incidental and occasional personal use that is infrequent or brief in duration is permitted so long as it occurs on personal time, does not interfere with District business, and is not otherwise prohibited by District policy or procedures.

Use of District Software: District software is licensed to the District by a large number of vendors and may have specific license restrictions regarding copying or using a particular program. Users of District software must obtain permission from the District prior to copying or loading District software onto any computer, whether the computer is privately owned or is a District computer.

Use of Non-District Software: Prior to loading non-District software onto District equipment a user must receive permission from the District. All software must be legally licensed by the user prior to loading onto District Equipment. The unauthorized use of and/or copying of software is illegal.
Users are not to delete or add software to District computers without District permission. Due to different licensing terms for different software programs, it is not valid to assume that if it is permissible to copy one program, then it is permissible to copy others.

Document Management and Storage: All documents related to the conduct of District business and all educational records identified in Policy 3231P Student Records, shall be stored on District provided systems and storage services.

Unacceptable/Prohibited Network Use by Staff Includes:

- Commercial Use: Using District network for personal or private gain, personal business, or commercial advantage is prohibited.

- Use of Personal Storage Services: Using any cloud or personally-acquired document management or storage service for district business 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 working 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 Entertainment Use: District Network may not be used for storage of personal entertainment/media files.

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, misdeliveries, 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.

Network Security

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 and for authorized district purposes. Staff 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 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.

Privacy

The District network, computers, internet, and use of e-mail are not inherently secure or private. Users are urged to be caretakers of your own privacy and to not store sensitive or personal information on District computers.

The District may monitor and review electronic information in order to analyze the use of systems or compliance with policies, conduct audits, review performance or conduct, obtain information, or for other reasons.

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. Backup is made of all district e-mail correspondence for purposes of public disclosure, disaster recovery, and records retention.

Care for District Computers

Staff users of District computers are expected to respect the District's property and be responsible in using the equipment. Users are to follow any District instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for District Computers under their control. The District is responsible for any routine maintenance or standard repairs to District computers. Users are expected to notify the District in a timely manner of the need for any service.

If a District laptop is lost, damaged, or stolen while under the control of a user, the user is expected to report such loss immediately to their supervisor.

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.

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 Staff Use of Electronic Resources policy or in the Acceptable Use Procedures (AUP) could be cause for disciplinary action, up to and including revocation of network and computer access privileges, restitution, discharge, and/or police report in accordance with District Staff Discipline Policies and Procedures.

Adopted:
09/01/19