

Electronic Resources and Internet Safety

K-20 Network Acceptable Use Guidelines/Internet Safety Requirements

These procedures are written to support the Electronic Resources Policy of the board of directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship includes the norms of appropriate, responsible, and healthy behavior related to current technology use. Successful, technologically-fluent digital citizens recognize and value the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world. They cultivate and manage their digital identity and reputation, and are aware of the permanence of their actions in the digital world. Expectations for student and staff behavior online are no different from face-to-face interactions.

Use of Personal Electronic Devices

In accordance with all district policies and procedures, students and staff may use personal electronic devices (e.g. laptops, mobile devices and e-readers) to further the educational and research mission of the district. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day. Absent a specific and articulated need (e.g. assistive technology), students do not have an absolute right to possess or use personal electronic devices at school.

Network

The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (websites including social networking). The district reserves the right to prioritize the use of, and access to, the network.

Acceptable network use by district students and staff include:

- A. Creation of files, digital projects, videos, web pages, and podcasts using network resources in support of education and research;
- B. Participation in all websites, including social networking, and the creation of content including podcasts, e-mail, and webpages that support education and research;
- C. With parental permission, the online publication of original educational material, curriculum-related materials, and student work. Sources outside the classroom or school must be cited appropriately;
- D. Students and staff use of the network for incidental personal use in accordance with all district policies and procedures; or
- E. Connection of any personal electronic device is subject to all procedures in this document and district policy.

Unacceptable network use by district students and staff includes but is not limited to:

Lynden School District No. 504
BOARD POLICY

Policy: 2022P

-
- A. Personal gain, commercial solicitation, and compensation of any kind;
 - B. Actions that result in liability or cost incurred by the district;
 - C. Support for or opposition to ballot measures, candidates, and any other political activity;
 - D. Hacking, cracking, vandalizing, the introduction of malware, including viruses, worms, Trojan horses, time bombs, and changes to hardware, software, and monitoring tools;
 - E. Unauthorized access to other district computers, networks, and information systems;
 - F. Action constituting harassment, intimidation or bullying, including cyberbullying, hate mail, defamation, discriminatory jokes, and remarks. This may also include the manufacture, distribution, or possession of inappropriate digital images;
 - G. Information posted, sent, or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
 - H. Accessing, uploading, downloading, storage and distribution of obscene, pornographic, or sexually explicit material
 - I. Attaching unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken; or
 - K. Any unlawful use of the district network, including but not limited to stalking, blackmail, violation of copyright laws, and fraud.

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 his/her 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

Personal Information and Inappropriate Content:

- A. Students and staff should exercise caution when providing personal information, on web sites, including social networking, e-mail, or as content on any other electronic medium;
- B. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
- C. No student pictures or names can be published on any public class, school or district website unless the appropriate permission has been obtained according to district policy;

-
- D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority; and
 - E. Students should be aware of the persistence of their digital information, including images and social media activity, which may remain on the Internet indefinitely.

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. The determination of what constitutes "other objectionable" material is a district decision.

- A. Filtering software is not 100 percent 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/her use of the network and Internet and avoid objectionable sites;
- B. E-mail inconsistent with the educational and research mission of the district will be considered SPAM and may be blocked from entering district e-mail boxes;
- C. 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 devices;
- D. 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
- E. The district may monitor student use of the district network, including when accessed on students' personal electronic devices and devices provided by the district, such as laptops, netbooks, and tablets.

Internet Safety Instruction

All students will be educated about appropriate online behavior, including interacting with other individuals on all website, including social networking websites.

- A. Age appropriate materials will be made available for use across grade levels; and
- B. Training on online safety issues and materials implementation will be made available for administration, staff, and families.

Copyright

Downloading, copying, duplicating, and distributing software, music, sound files, movies (including streaming services), 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 is permitted when such duplication and distribution falls within the [Fair Use Doctrine](#) of the United States Copyright Law ([Title 17, USC](#)) and content is cited appropriately.

Ownership of Work

All work completed by employees as part of their employment will be considered property of the district. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the district, the work will be considered the property of the district. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

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 and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

- A. Change passwords according to district policy;
- B. Do not use another user's account;
- C. If you write down your user account password, keep it in a secure location;
- D. Lock the screen or log off if leaving the computer.

Student Data is Confidential

District staff must maintain the confidentiality of student data in accordance with the [Family Educational Rights and Privacy Act \(FERPA\)](#).

No Expectation of Privacy

The district provides the network system, e-mail, and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review, and store, without prior notice, information about the content and usage of:

- A. The district network, including when accessed on personal electronic devices and on devices provided by the district, such as laptops, netbooks, and tablets;
- B. User files and disk space utilization;

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

No student or staff user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Archive and Backup

Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Refer to the district retention policy for specific records retention requirements.

Disciplinary Action

All users of the district's electronic resources are required to comply with the district's policy and procedures (and agree to abide by the provisions set forth in the district's user agreement). Violation of any of the conditions of use explained in the district's user agreement, Electronic Resources policy, or in these procedures could be cause for disciplinary action as noted below:

- A. Student Disciplinary Action
 - suspension, expulsion, or emergency removal from school and suspension or revocation of network and computer access privileges.
- B. Staff Disciplinary Action:
 - will be subject to progressive discipline.

Accessibility of Electronic Resources

Federal law prohibits people, on the basis of disability (such as seeing and hearing impairments), from being excluded from participation in, being denied the benefits of, or otherwise being subjected to discrimination by the district. To ensure that individuals with disabilities have equal access to district programs, activities, and services, the content and functionality of websites associated with the district should be accessible. Such websites may include, but are not limited to, the district's homepage, teacher websites, district-operated social media pages, and online class lectures.

District staff with authority to create or modify website content or functionality associated with the district will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities. Any such staff member with questions about how to comply with this requirement should consult with the Director of Technology.

Lynden School District No. 504
BOARD POLICY

Policy: 2022P

Revised: June 17, 1999

Revised: June 23, 2005

Revised: May 26, 2011

Revised: March 22, 2012

Revised: February 8, 2024