Electronic Resources and Internet Safety

Acceptable Use Guidelines/Internet Safety Requirements
These procedures are written to support the Electronic Resources and Internet Safety 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 recognize that information posted on the Internet can have a long-term impact on an individual's life and career. 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
The district provides electronic devices to ensure staff can perform their jobs and students can accomplish learning objectives. It is the district's expectation that district-issued devices are used in accordance with all district policies and procedures. In addition, staff and students may use personal electronic devices (e.g. laptops and mobile devices) 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 (blogs, websites, collaboration software, social networking sites, wikis, etc.). The district reserves the right to prioritize the use of, and access to, the network.

All use of the network, as well as any materials stored, transmitted, or published on the system, must be in conformity to state and federal law-including FERPA and CIPA and district policy.

From time to time, the district may determine whether specific uses of the network are consistent with the regulations stated in this procedure. Under prescribed circumstances, non-student or staff use may be permitted, provided such individuals adhere to district guidelines for acceptable use.

For security and administrative purposes, the district reserves the right for authorized personnel to review system use and file content including, without limitation, the contents of district-provided personal and shared file storage, web browsing history on a district device and/or the district network, and district email.

Acceptable network use by district students and staff must comply with district guidelines, and may include:

A. Creation of files, digital projects, videos, web pages, and podcasts using network resources in support of education and research;

B. Participation in blogs, wikis, bulletin boards, social networking sites and groups as permitted under district filtering limitations, and the creation of content for 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. Downloading and installing games, audio files, video files, or other applications (including shareware or freeware) with approval and permission from the district IT and Teaching and Learning leadership;

E. Staff use of the network for incidental personal use in accordance with all district policies and procedures.

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

A. Actions that result in liability or cost incurred by the district;

B. Support for or opposition to ballot measures, candidates, and any other political activity;

C. Hacking, cracking, vandalizing, the introduction of malware, including viruses, worms, Trojan horses, time bombs, and changes to hardware, software, and monitoring tools;

D. Making use of the electronic resources in a manner that serves to disrupt the operation of the system by others, including modifying, abusing, or destroying system hardware, software, or other components;

E. Attempting to gain or achieving unauthorized access to other district computers, networks, and information systems;

F. Action constituting or contributing to 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 may be confiscated, and additional disciplinary action may be taken; or

J. 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

As our students engage with educational technology, it becomes increasingly necessary to model and explicitly teach digital citizenship and online safety. Ensuring that students understand how to wisely use technology and navigate media is an essential skill for our learners to be productive in life and learning. Safe online behavior should frequently be part of classroom discussion, teaching the learner how to use technology in meaningful, productive, respectful, and appropriate ways in their school life and personal life. In the Lynden School District, digital citizenship and online safety are explicitly taught by district staff, guest speakers, and law enforcement. The classroom is not the only place where digital citizenship should be discussed and modeled; it is important for the community and parents to be involved and remain educated in this discussion.

Staff will be educated regarding cybersecurity, including regular cybersecurity training as well as ongoing phishing simulations.

Personal Information and Inappropriate Content:

A. Students and staff should be cautious when providing personal information, including a home address and phone number on websites, blogs, podcasts, videos, social networking sites, wikis, 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 facing 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;

E. No user may use, disclose, or disseminate personally identifiable information of a minor without explicit parent/guardian permission;

F. Staff must follow district data-handling procedures, including 3231 – Student records, when handling any student's personally identifiable information; and

G. 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 content that is obscene as well as 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 local decision and determined by district-level leadership with input from district staff.

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. Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to district browser settings, and any other techniques designed to evade filtering or enable the publication of inappropriate content);

C. E-mail inconsistent with district guidelines may be considered SPAM and blocked from entering district e-mail boxes;

D. 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;

E. 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 ensure that student use conforms to district guidelines;

F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively;

G. The district may monitor staff and student use of the district network, including when accessed on personal electronic devices and devices provided by the district, such as laptops, netbooks, and tablets;

H. The district may block or delete any malicious content detected, and

I. The district will provide a procedure for staff members to request access to internet websites blocked by the district's filtering software. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request.

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 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
Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized user for authorized district purposes. Students and staff are responsible for all activity on their account and should:

A. Lock the screen or log off if leaving the computer (for those users with this level of computer permission);

B. Change passwords according to district policy/rules;

C. Protect online accounts from unauthorized use;

D. Keep account passwords confidential and safe

Privacy

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, regardless of how accessed;

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.

Hardware, Educational Applications, and Programs
Hardware, and all applications, including software, and operating systems must be approved for use prior to purchase and installation according to current technology purchase procedures. The district may remove any hardware, application, software, or operating system that does not meet these criteria.

Archive and Backup
Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up regularly.

Artificial Intelligence

Artificial Intelligence is a rapidly advancing set of technologies for capturing data to detect patterns and automate decisions. Artificial Intelligence (AI) has become an increasingly important part of our lives, and it is essential for students to understand when and how to use it

effectively and ethically. AI tools can enhance classroom learning, and their implementation should be guided with proper training, ethical considerations, and responsible oversight. When utilizing generative AI tools to create or support the creation of texts or creative works, students are expected to adhere to guidance provided by their classroom teacher.

A. Purpose

While the district is not in the fiscal position to provide paid AI licensure for all staff and students, the district will permit staff and student access to approved, generative Artificial Intelligence tools that are cost-free. The district will maintain a list of approved AI tools that is readily accessible to all staff via the district intranet. Approved AI tools will be implemented for the following purposes:

- Providing students with an opportunity to engage in current technologies in a learning environment, to better prepare them for the world they will live and work in.
- Extending the benefits of these tools to the workplace, where appropriate.

B. Appropriate Use

Student and staff use of generative Artificial Intelligence technologies should be used to support and extend student learning and workplace productivity.

C. Inappropriate Use

In addition to those uses that violate this procedure the following are prohibited uses of Artificial Intelligence:

- Any use of Artificial Intelligence that does not align with expectations outlined by a classroom instructor or building administrator. It is ultimately the teacher's responsibility to determine the appropriate level of use of Artificial Intelligence in each classroom, and for each assignment or project.
- Use of Artificial Intelligence to complete an assignment in a way that represents the assignment as one's own work.
- Use of Artificial Intelligence to purposefully create misinformation or to misrepresent others for the purpose of harming or bullying groups or individuals.
- Use of Artificial Intelligence with confidential student or staff personal information. Exceptions are granted to staff using protected licensure that has been provided by the Lynden School District or by the individual employee, once approved in writing by IT and Teaching and Learning leadership.

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, as well as associated documents. Violation of any of the conditions of use explained in any of these documents could be cause for suspension or revocation of network, computer access, or other electronic resources privileges. Additionally, violations of these documents could result in disciplinary action, including suspension from school, termination of employment, and/or civil or criminal actions, as warranted.

Accessibility of Electronic Resources
In compliance with federal and state law, all District-sponsored programs, activities, meetings, and services will be accessible to individuals with disabilities, including persons with hearing, vision, and/or speech disabilities. To ensure such, 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, 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 staff member with questions about how to comply with this requirement should contact the Lynden School District central office.