Electronic Resources 2017-2018

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 represents more than technology literacy. Successful, technologically-fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the internet is public and permanent and can have a long-term impact on an individual's life and career. 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. District staff will retain the final authority in deciding when and how students and staff may use personal electronic devices on school grounds and during the school day.

A personal computing device (PCDs) is defined as an electronic communication device capable of internet access, word processing, and other school-related applications. These could include the following: laptop, net book or tablet computer, e-reader, or any other personal computing devices that may be stand-alone or may use wireless communications between users across some form of telecommunications network.

The use of personal computing devices on campus is a privilege, which the District grants to any student and staff who is willing to assume the responsibility of abiding by the guidelines set forth in this document. All policies and procedures set in place in the Acceptable Use Policy/Procedure (AUP) continue to apply when the student and staff uses their personal computing devices on campus.

Management and Supervision of Personal Computing Devices. There will be no expectation that students and staff will be required to bring personal computing devices to school.

The LaCrosse School District assumes no responsibility or financial liability for any damage the student or parent suffers, including but not limited to theft, physical damage, loss of data, or software malfunctions of the personal computing device. If a personal computing device appears to have been stolen, the student and staff will immediately report the incident to school administration who will contact the authorities if warranted.

Permission for using and charging of the personal computing devices in any instructional area, including but not limited to classrooms, will be at the discretion of the supervising adult and/or classroom teacher and school administration.

Use of personal computing devices in designated common areas will be allowed but subject to the restrictions stated in the District policies and by administration. If a student or staff appears to be in violation of any District policy, they should refer the violation to a school or district administrator.

Appropriate Use Students are to use these devices in a responsible, efficient, ethical, and legal manner for educational purposes only. School policy may further define acceptable student use of

the PCDs. The teacher/administration reserves the right to determine if a student's use of a personal computing device is inappropriate and/or disrupts the learning environment and may take appropriate disciplinary action, including but not limited to confiscation of the device, which will be returned to the student and/or parent(s)/guardian(s) in accordance with established building guidelines. In order to insure adequate bandwidth, students may only use PCDs for educational purposes. The District does not take responsibility for technical support for any personally owned device used at school. Directions for connecting to the District's guest network will be provided.

Students and staff may only connect PCDs to the specific wireless network. This network will provide access to the internet, including all publicly available LaCrosse School District resources. Connecting a PCD to a wired network, or any other available LaCrosse School District wireless network is prohibited student and staff use of the District's wireless network is bound by the District's Acceptable Use Policy/Procedure 2022. Personally owned devices used in school are not permitted to connect to the internet through a 3G, 4G, or other content service providers. Personally owned devices must access the internet via the District's content filtered wireless network (guest access).

All District students shall review this Policy and associated technology guidelines and have a signed parent consent form on file before students utilize personally owned devices. The District reserves the right to restrict student use of district owned technologies and personally owned devices on school property or at school-sponsored events. If a student or staff is suspected of violating the terms of the Policy, the administration will determine the appropriate course of action, including but not limited to:

o Revoking PCD Internet connectivity for the student or staff; o Searching the electronic device and the records on student and staff technology

equipment in accordance with Student Privacy and Searches Policy 3230 and maintaining

safety, order, and discipline; o Prohibiting the PCD from being brought on campus; o Prohibiting PCD use in specific locations or settings; o Assigning standard disciplinary consequences as listed in the Student Handbook.

Network

The District network includes wired and wireless devices, 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 must support education and research and be consistent with the mission of the District.

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. Participationinapproved(determinedbyajointdecisionofadministrationand technology department) blogs, wikis, bulletin boards, social networking sites, and groups and the creation of content for podcasts, e-mail and webpage's that support education and

research;

C. Withparentalpermission,theonlinepublicationoforiginaleducationalmaterial, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;

D. Staff use of the network for incidental personal use in accordance with all District policies and procedures; or

E. Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the District network after checking to confirm that the device is equipped with up-to-date virus software, compatible network card and is configured properly. Connection of any personal electronic device is subject to all procedures in this document and will be determined on an individual basis.

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

A. Personal gain, commercial solicitation, and compensation of any kind;

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

C. Downloading,installinganduseofaudiofiles,videofiles,gamesorotherapplications (including shareware or freeware) without permission or approval from the technology department and administrator;

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

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

F. Unauthorized access to other district computers, networks and information systems;

G. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes, and remarks;

H. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);

I. Accessing, uploading, downloading, storage and distribution of obscene, pornographic, or sexually explicit material; or

J. Attaching unauthorized devices to the District network. Any such device may confiscated and additional disciplinary action may be taken.

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 not reveal personal information, including a home address and phone number on web sites, 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 written 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; and

D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

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 will be filtered. The determination of what constitutes "other objectionable" material is a local decision but is no less than required by CIPA and district policy.

A. Access by minors to inappropriate matter on the internet;

B. The safety and security of minors when using electronic mail, chatrooms, and other forms of direct electronic communications;

C. Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;

D. Unauthorized disclosure, use, and dissemination of personal information regarding minors; and

E. Measures restricting minors' access to materials harmful to them.

F. 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;

G. 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);

H. E-mail inconsistent with the educational and research mission of the District will be considered

SPAM and blocked from entering District e-mail boxes;

I. 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;

J. 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

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

Internet Safety Instruction All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.

A. Age appropriate materials will be made available for use across grade levels.

B. Trainingononlinesafetyissuesandmaterialsimplementationwillbemadeavailablefor administration, staff, and families.

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 written permission prior to distributing his/her work to parties outside the school.

Network Security and Privacy

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 for authorized District purposes. Students and staff are responsible for all activity on their account and should 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 **or share your user account with others;**

C. Do not insert passwords into e-mail or other communications;

D. If you write down your user account password, keep it in a secure location;

E. Do not store passwords in a file without encryption;

F. Do not use the "remember password" feature of internet browsers; and

G. Lock the screen or log off if leaving the computer.

H. Report immediately if your user account or other user's accounts have been compromised.

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 network;

B. User files and disk space utilization;

C. User applications and band width 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 or other 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. Barring power outage or intermittent technical issues, staff, and student files are backed up on District servers regularly. 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 Acceptable Use Policy/Procedure (AUP) 2022, Electronic Resources policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Students who are found violating Acceptable User Policy will be considered to have committed a violation in one or both of two categories: Internet Violation or Network Violation. Typical punishments for Internet Violations include but are not limited to: Removal of internet on first offense for a period determined by on-site Administration second offense, longer removal of internet access, possible loss of network privileges and conference with Legal Guardian(s), total loss of network and internet access for remainder of current school year, as well as discipline decided by school Administration. Typical punishments for Network Violations include but are not limited to: Removal of all network access for a period determined by on-site Administration for first offense, second offenses typically removal of network access for a extended period possible conference with legal Guardian(s), and third offense, total removal of Network privileges for rest of year and disciplinary action.

STUDENT ACCESS TO NETWORKED INFORMATION RESOURCES

The **LaCrosse School District** is pleased to offer our students access to the district computer networks for electronic mail and the Internet. To gain access to e-mail and the Internet, all students under the age of 18 must obtain parental permission and must sign and return this form to the Technology Director. Students 18 and over may sign their own forms.

Access to e-mail and the Internet will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. Families should be warned that some materials accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make the Internet access available to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the LaCrosse School District supports and respects each family's right to decide whether or not to apply for access.

District Internet and E-Mail Rules

- Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply.
- The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parent permission is required. Access is a privilege-not a right. Access entails responsibility and users waive any rights to privacy, which they would otherwise have regarding such material. All network activity and content will be filtered to the best of the district's ability.
- Individual users of the District computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with District standards and will honor the agreements they have signed. Beyond the clarification of such standards, the district is not responsible for restricting, monitoring or controlling the communications of individuals utilizing the network.
- Network storage areas may be treated like school lockers. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should expect that files stored will not be private and will be filtered through district network filtering.
- Within reason, freedom of speech and access to information will be honored. During school, teachers of younger students will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.
- As outlined in **Board policy** and **procedure 2022** on students rights and responsibilities, the following are some examples of the things not permitted and considered Network and Internet Offenses:
  - Sending or displaying offensive messages or pictures
  - Using obscene language
  - Harassing, insulting or attacking others
  - Damaging computers, computer systems or computer networks
  - Violating copyright law
  - Using another's password
  - Trespassing in another's folders, work or files
  - Intentionally wasting limited resources
  - Employing the network for commercial purposes
  - Bypassing or sabotaging security and filtering measures set in place by the District.
  - Attaching any unauthorized equipment to the network.

***NOTICE:* Violations of Network and Internet offenses may result in a loss of access as well as other disciplinary or legal action.**

User Agreement and Parent Permission Form

As a user of the LaCrosse School District computer network, I hereby agree to comply with above rules - communicating over the network in a reliable fashion while honoring all relevant laws and restrictions.

_____ _____ _____

STUDENT LEGAL NAME *(print)* STUDENT SIGNATURE DATE

_____ _____ _____

PARENT NAME *(print)* PARENT SIGNATURE DATE

I have read this form and do NOT want my child to have Internet Access: _____

Please Sign and return to the Technology Director *Initial Here*