Enumclaw SCHOOL DISTRICT
all students achieving at high levels

Responsible Use Procedure:
Electronic Resources and Internet Safety
Student Summary

The Enumclaw School District Board of Directors recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The board also believes that staff and students need to be proficient and safe users of information, media, and technology to succeed in a digital world. The district's technology will enable educators and students to communicate, learn, share, collaborate and create; to think and solve problems; to manage their work; and to take ownership of their lives.

This document is a summary of the rules, guidelines, personal safety recommendations and code of conduct as stated in the *Responsible Use Procedure: Electronic Resources and Internet Safety* (2022P).

Responsible 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 blogs, wikis, bulletin boards, social networking sites and groups 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. Connection of any personal electronic device is subject to all procedures in this document.

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, installing and use of games, audio files, video files, games or other applications (including shareware or freeware) on district-owned devices or equipment without permission or approval from the Technology Operations Leader;
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; (If students encounter digital harassment, intimidation, or bullying, they should notify the appropriate school authority);
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 will be confiscated and additional disciplinary action may be taken.

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 must not share their account password.

The following procedures are designed to safeguard network user accounts:

A. Do not use another user's account;
B. Do not insert passwords into e-mail or other communications;
C. If you write down your user account password, keep it in a secure location;
D. Do not store passwords in a file without encryption;
E. Do not use the "remember password" feature of Internet browsers; and
F. Lock the screen or log off if leaving the computer.

Internet Safety

A. 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.
B. Students and staff should not reveal 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;
C. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.
E. Students should never make appointments to meet people in person that they have contacted online without adult permission.

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.

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.

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 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.

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, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.