Procedure - Electronic Resources and Internet Safety

K-20 NETWORK 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 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.

It is assumed that parents grant their child the right to access the network and have a desire to have their child use network resources which include the Internet as an educational resource unless their school has a signed Internet and Electronic Communication Exclusion form on file.

Use of the computer network and Internet is a privilege. A user who violates this agreement shall, at a minimum, have their access to the network temporarily terminated. The district may also take other disciplinary actions up to and including termination of employment or expulsion from 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 must be in conformity to state and federal law, network provider policies and district policy.

All use of the network must support education and research and be consistent with the mission of the district. From time to time, the district will make a determination on 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 demonstrate that their use furthers the purpose and goals of the district.

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.

A. The use of personal devices on the district network is subject to available resources and may be restricted from some network resources.

B. The owner of these devices must ensure that the district and student data are adequately protected. The district reserves the right to issue guidelines for data protection. Protection requirements may include password protection for access to the device, data encryption and applications that can remotely remove all data from a device that has been lost or stolen.

C. All personal electronic devices (wired or wireless) including portable devices connected to the district's network must be equipped with up-to-date virus software, compatible network card and be configured properly. Connection of any personal electronic device is subject to all guidelines in this document.

D. For security and administrative purposes, the district reserves the right for authorized personnel to review system use and file content including, without limitation, the content of any district email. Email is archived as per Public Disclosure Laws.

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 directives are designed to safeguard network user accounts:

A. Change passwords according to district policy;

B. Do not use another user's account;

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

D. Keep user account passwords in a safe location if written down;

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.

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 blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, email and web pages 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; and

D. 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. 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) that do not support the educational mission;

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

G. Contributing to 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, storing and distributing obscene, pornographic or sexually explicit material;

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

K. 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.

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 their 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 websites, blogs, podcasts, videos, social networking sites, wikis, email 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 may 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 could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

A. Filtering software is not 100% 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 their 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 the educational and research mission of the district will 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 the mission and goals of the district.

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

G. The district will provide a procedure for staff to request access to internet websites blocked by the district's filtering software. The procedure will indicate a timeframe for a designated school official to respond to the request. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request as well as disruption to the classroom environment. The district will provide an appeal process for requests that are denied.

Internet Safety Instruction

All students will be educated regarding appropriate digital citizenship including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

A. Each school will create a Digital Citizenship Plan which will identify the content taught at each grade level, by whom and when.

B. Training regarding 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, 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 district or unless such work has been paid for under a written agreement with the district. 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 the student's work to parties outside the school.

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 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. 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 Electronic Resources and Internet Safety policy and procedure 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 and Internet Safety policy or in this procedure could be cause for disciplinary action, including suspension or expulsion from school or termination of employment and suspension or revocation of network and computer access privileges. In addition, violations of this policy may result in criminal prosecutions, if warranted.

Adoption Date: 04.05.96
Edmonds School District
Classification: Priority
Revised Dates: 06.04.02; 01.10.06; 06.20.06; 10.20.12; 06.13.18; 07.13.18