Procedure - Electronic Resources and Internet Safety

Toppenish School District 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. 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.

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 support education and research and be consistent with the mission of the district.

Public Records
Because Toppenish Public Schools is a public agency under the Washington Public Records Act, chapter 42.56 RCW, any information or record relating to the conduct of government or the performance of any governmental: functions that is prepared, owned, used, or retained by the district is a public record subject to disclosure upon request by any person. Such information may include retained records related to communications by or through district resources or records of Internet activity accessed by or through district resources. Whether such records, or any portion of such records, fall within the narrow exemptions of the Public Records Act will be determined once a request is received.

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, 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 and all copyright laws must be followed;

D. Participation in district sponsored social media to inform and communicate with members of the school district community consistent with the education mission of the District and in compliance with District policy and procedure;

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

F. Participation in district sponsored social media to inform and communicate with members of the school district community consistent with the education mission of the District and in compliance with District policy and procedure;

G. Connection of no more than two personal electronic devices (wired or wireless) including portable devices with network capabilities to the district network, after *checking with* the Coordinator of Operational Technology, 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; or

H. Use of electronic resource accounts solely by the authorized owner of the account for the authorize purpose.

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

A. Any use of the electronic resources for individual profit or gain; for fundraising activities without prior approval of the Administration; for political action or political activities; or for excessive personal use. "Political action or political activities" includes support of or opposition to political campaigns, candidates, ballot measures, or lobbying for or in opposition to legislation;

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

C. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner other than use that falls within the scope of "reasonable fair use." The "Fair Use Doctrine" of the United States Copyright Law (Title 17, USC) permits the duplication and/or distribution of materials for educational purposes under most circumstances. Questions regarding whether the duplication or distribution of copyrighted materials violates federal law should be directed to the Instructional Technology Office;

D. Downloading, installing and use of games, audio files, video files, games or other applications (including shareware or freeware) without permission or approval from the Coordinator of Operational Technology or the Director of Instructional Technology;

E. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools, and malicious use of the electronic resources to develop programs that harass other users, infiltrate a computer or computing system, and/or damage the software components of a computer or computing system;

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

G. Any attempts to defeat or bypass the District's Internet filtering technologies by using or trying to use proxies, https, special ports, modification to District browser settings, or any other techniques, designed to avoid being blocked from inappropriate content or to conceal Internet activity;

H. Contributing to cyberbullying, chain-letters, hate mail, defamation, harassment, intimidation, denigrating comments, discriminatory jokes and remarks of any kind, and other similar conduct;

I. Using or forwarding profanity, obscenity, vulgar language, racist terms, or other language that is offensive to a reasonable person;

J. Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or misrepresenting other users using electronic resources;

K. Using an electronic account authorized for another person;

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

M. Accessing, uploading, downloading, storage and distribution of transmit obscene or pornographic content, sexually inappropriate content, or files dangerous to the integrity of the network;

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

O. Using any electronic resource for unlawful purposes.

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.

Staff Responsibilities

A. Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment shall make reasonable efforts to monitor the use of this equipment to assure that use or activity conforms to electronic resources procedures and is consistent with the mission and goals of Toppenish Public Schools.

B. Staff should make reasonable efforts to become familiar with the electronic resources and their use so that effective monitoring, instruction, and assistance may be provided. Staff should report any misuse to their supervisor.

Toppenish Public School’s Responsibilities

Toppenish Public Schools recognizes its obligation to both protect the well-being of students in its charge and to be the steward of public property and resources. To these ends, the district reserves the right to, and may at any time, do the following:

- Log electronic resource use and monitor cloud, email, or fileserver space utilization by users. The District assumes no responsibility or liability for files deleted due to violation of storage allotment
- Monitor the use of activities through the District's networks and electronic resources. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.
- Provide internal and external controls as appropriate, including the right to determine who will have access to Toppenish Public Schools-owned equipment.
- Restrict or exclude those who do not abide by Toppenish Public Schools' electronic resources policy or other policies governing the use of school facilities, equipment, and materials.
- Report to appropriate authorities apparent violations of the law discovered through the District’s monitoring of electronic resources
- Restrict electronic resource destinations through software or other means.
- Provide guidelines and make reasonable efforts to train staff and students in acceptable use and policies governing electronic resource communications.
- Monitor and maintain mailing list subscriptions and delete files from the personal mail directories to avoid excessive use of fileserver storage space.
- Use filtering software or technologies to block or filter access to visual depictions that are obscene and all child pornography in accordance with CIPA. Other objectionable material may likewise be filtered. The determination of what constitutes "objectionable" material is determined by the District's administration consistent with the District’s educational mission, the district’s policies and procedures, and the goals. Requests for blocked content evaluation or temporary filtering bypass shall be directed to the Library Media Specialist local to a school site or to the Educational Technology Department.

Legal Notices

A. Toppenish Public Schools is not responsible for the information that is retrieved via electronic resources.

B. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. Educational Technology staff have access to all email and will monitor messages.

C. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

D. The District reserves the rights to monitor, inspect, copy, review, and store without prior notice any and all usage of:
   - The network
   - User files and disk space utilization
   - User applications and bandwidth utilization
   - User document files, folders, and electronic communication

- Email
- Internet access
- Any and all information transmitted or received in connection with network and/or email use operated by or through District resources

E. All information files shall be and remain the property of the District, and no student or staff user shall have any expectation of privacy regarding such materials. The District reserves the right to disclose any electronic message to law enforcement officials or third parties as deemed appropriate. All documents generated, received, transmitted, or maintained through district resources or networks are subject to the disclosure laws of the State of Washington's Public Records Act, chapter 42.56 RCW.

F. Archives are maintained of email for the purpose of public disclosure requests and disaster recovery. Barring power outage or intermittent technical issues, backups are made of staff and student files on District servers for recovery of accidental loss of deleted files. Recovery is not guaranteed.

G. While filtering software makes it more difficult for objectionable material to be received or accessed through district resources, filters are not infallible. The ability to access a site does not mean that otherwise objectionable material or an objectionable site falls within the district's acceptable use requirements. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites and/or materials. Any inadvertent visit to an objectionable site must be reported immediately.

H. From time to time, Toppenish Public Schools will make determinations on whether specific uses of electronic resources are consistent with the Electronic Resources policy.

I. Toppenish Public Schools will not be responsible for any damages users may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or user errors or omissions. Use of any information obtained is at the user's own risk.

J. Toppenish Public Schools makes no warranties (expressed or implied) with respect to:
   - The content of any advice or information received by a user or any costs or charges incurred as a result of seeking or accepting any information.
   - Any costs, liability, or damages caused by the way the user chooses to use his or her access to the electronic resources.

K. Toppenish Public Schools reserves the right to change its rules and procedures at any time without notification.

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 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.

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 cyberbullying awareness and response:

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.

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 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 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 assure that student use conforms to the mission and goals of the district; and

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 students and staff members to anonymously 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. The district will provide an appeal process for requests that are denied.

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 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. 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.

Student Data is Confidential
District staff must at all times maintain the confidentiality of student data in accordance with district policy, the Family Educational Rights and Privacy Act (FERPA). And the Health Insurance Portability and Accountability Act ("HIPAA"), and corresponding state law.

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.

Personal Device Warning

A. By connecting a mobile device to Toppenish Public Schools email system, you acknowledge and agree that Toppenish Public Schools Educational Technology Department reserves the right to enforce any reasonable security measures deemed necessary to mitigate data leakage and protect students. This includes but is not limited to:
   - Remotely deleting the contents of your mobile device when deemed necessary, e.g., when a password is incorrectly entered more than 10 times. The deletion may include district and personal contacts, pictures, etc.
   - Enforcing the use of a password *I* pin to access the mobile device.
   - Restricting the use of applications deemed a security risk.

B. In addition, users of district networks with personal devices understand that documents of records prepared, owned, used, or retained by any local or public agency – including the electronic communications of a public agency – are public records under Washington State law. Using any personal device or computer for school district business can result in a requirement that you submit your personal device for examination or search if a public records request is received concerning information related to governmental conduct or the performance of any governmental function that may be stored on your personal device.

C. The mobile devices that are subject to this policy are those that are directly connected to Gmail via the Google API.

D. Examples of Google enabled devices include but are not limited to: iPhone, iPod, iPad, Android based mobile phone, tablet device, Windows based mobile phone, etc.

Violations of Acceptable Use

A. Any reasonable belief that user activity has violated this policy and procedure regarding acceptable use should be reported to the school, program, or department administrator responsible for supervision of the use in question. Disciplinary action, if any, for students, staff, and/or other users shall be consistent with the District's policies and procedures.

B. Violations of this policy can constitute reasonable cause for the limitation or revocation of access privileges, suspension of access to Toppenish Public Schools electronic resources. Violations may also result in employee discipline for staff or school disciplinary action for students, as well as other appropriate legal or criminal sanctions, as appropriate.

C. Challenging the Denial or Restriction of Access to District Electronic Resources

D. If a person is denied access or subject to restricted access to the District's electronic resources resulting from a determination that the person has violated the District's acceptable use standards, the denial or restriction may be appealed in the manner described below:
   - If access to electronic resources is denied or restricted for an employee, reconsideration of that action may be requested in accordance with appropriate District policies governing discipline, or through the grievance process in accordance with the terms of the staff member's collective bargaining agreement.
   - If access to electronic resources is denied or restricted for a student, the denial or restriction may be grieved or appealed consistent with the procedures for student corrective action in Chapter 392-400 WAC applicable to the discipline, suspension or expulsion being imposed.

Adoption Date:
Classification:
Revised Dates: **06.01; 06.08; 06.11; 02.12; 06.15**

STUDENT ACCEPTABLE USE POLICY AND PARENT OPT-OUT FORM

Introduction

We are pleased to offer students of the Toppenish Public Schools access to the district computer network resources, electronic mail and the Internet. Parents, please review this document carefully, with your son/daughter. Families have the right to restrict the use of Internet and e-mail by completing this form and returning it to your school. The request for restriction is recorded in the student information system, and the form is kept on file. Any questions or concerns about this permission form or any aspect of the computer network should be referred to the Toppenish School District Technology Department.

OPT-OUTS remain in effect for the current school year.
If no documentation is on file, it will be assumed that permission
for Internet and e-mail usage has been granted.

General Network Use

The network is provided for students to conduct research, complete assignments, and communicate with others. Access to network services is given to students who act in a considerate and responsible manner. Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Access is a privilege-not a right-and entails responsibility. As such, general school rules for behavior and communications apply and users must comply with district standards. Beyond the clarification of such standards, the district is not responsible for restricting, monitoring or controlling the communications of individuals utilizing the network.

District staff may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on district servers will be private.

Internet/E-mail Access

Access to the Internet and e-mail will enable students to use thousands of libraries and databases. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. Filtering software is in use, but no filtering system is capable of blocking 100% of the inappropriate material available on the Internet. 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. 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 Toppenish Public Schools supports and respects each family's right to decide whether or not to restrict access.

STUDENT ACCEPTABLE USE POLICY AND PARENT OPT-OUT FORM

Unacceptable network use includes but is not limited to:

- Sending, storing or displaying offensive messages or pictures;
- Using obscene language;
- Giving personal information, such as complete name, phone number, address or identifiable photo, without permission from teacher and parent or guardian;
- Cyberbullying, hate mail, harassing, insulting or attacking others, discriminatory jokes and remarks;
- Damaging or modifying computers, computer systems or computer networks: downloading, installing and using games, audio files, video files or other applications including shareware or freeware;
- Violating copyright laws;
- Sharing or using others' logons or passwords or other confidential information;
- Trespassing in others' folders, work or files;
- Intentionally wasting limited resources;
- Posting information, sent or stored, online that could endanger others;
- Employing the network for nonacademic, personal, commercial, political purposes, financial gain, or fraud;
- Attaching unauthorized equipment to the district network.

Violations may result in a loss of access (Administrative Policy and Procedures 3200, Student Rights and Responsibilities; Policy 2022, Electronic Resources). Additional disciplinary action may be determined at the school level. When applicable, law enforcement agencies may be involved.

Parent/Guardian Opt Out:

Check below if you **DO NOT** want your student to have access to one or more of the following:
___ E-mail systems
___ Internet

OPT OUTS remain in effect for the current
school year.
If no documentation is on file, it will be assumed that permission has been
granted for access to the Internet and e-mail usage.

Student Name ______________________________School________________Grade

____

Parent/Guardian Signature_________________________________Date

____

Please return this form to your school office.