Electronic Resources

Staff Acceptable Use Agreement

This Staff Acceptable Use Agreement is written to support district Policy 2035 – *Electronic Resources*, and accompanying Procedure P2035-1 – *Electronic Resources Procedures*.

Network

The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and internet content (blogs, web sites, 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 staff includes:

- Creation of files, digital projects, videos, web pages and podcasts using network resources in support of education and research;
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support education and research;
- 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;
- Staff use of the network for incidental personal use in accordance with all district policies and procedures;
- Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities (phones, tablets) to the district network must be approved and processed through the Riverview Technology Department. Connection of any personal electronic device is subject to all procedures in this document.

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

- Personal gain, commercial solicitation and compensation of any kind;
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material;
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan Horses, time bombs and changes to hardware, software and monitoring tools;
- Causing or attempting to cause security breaches or disruptions of network communication and/or network performance
- Unauthorized access to other district computers, networks and information systems;
- Downloading, installing and use of games, audio files, video files or other applications (including shareware or freeware) without permission or approval from the Riverview Technology Department;
- Attaching unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken;

- Support for or opposition to ballot measures, candidates and any other political activity;
- Actions that result in liability or cost incurred by the district;

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:

- Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission.
- Staff will not interact with students in a personal manner on Internet social networking sites such as Facebook, Twitter, or any similar sites.
- No student pictures or names can be published on any public class, school or district web site unless the appropriate permission has been obtained according to district policy.
- Offensive, objectionable, inappropriate content, or content inconsistent with district policies, posted on District-owned or operated internet sites or pages will be deleted at the discretion of the Superintendent or designee.

Social Networking

The Riverview School District recognizes that social media is a tool that can be used to promote and enhance its education and communication goals. The District's use of social media is limited to promoting the mission and goals of the District. The District's electronic resources may include District established social medial sites or accounts, such as Facebook pages, Twitter, or other similar interactive media that allow members of the public to post material onto sites created and maintained by the District. Policy 2036 and Procedures P2036-1 apply to members of the public accessing such sites, and any violation of these requirements will result in removal of prohibited content and/or denial of access privileges for violators.

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.

- 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 his or her use of the network and internet and avoid objectionable sites;
- Any attempts to defeat or bypass the district's internet filter or conceal internet activity are prohibited: proxies, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;
- E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
- 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;
- 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
- Staff must make a reasonable effort to become familiar with the internet and to monitor, instruct and assist effectively.
- 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 request 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 are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

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.

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 must not share their account password.
The following procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your user account password, keep it in a secure location;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of internet browsers; and
- Lock the screen, or log off, if leaving the computer.

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:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and
- 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 on a regular basis. Refer to the district retention policy for specific records retention requirements.

In order to comply with laws on public disclosure, archival requirements, and records retention, all official district business in electronic form shall be conducted only on approved district systems. This includes wikis, blogs, email, web sites, and other similar electronic records and communications.

Disciplinary Action
All users of the district's electronic resources are required to comply with district Policy 2035 – *Electronic Resources*, and accompanying Procedure P2035-1 – *Electronic Resources Procedures*. Violation of any of the conditions of use explained in the district's Electronic Resources policy or in these procedures could be cause for disciplinary action, including suspension or revocation of network and computer access privileges, and up to termination of employment.

Staff Acceptable Use Agreement for District Electronic Resources

I understand that all technology related equipment, computers, software, online resources, network and account access provided by the Riverview School District are for educational purposes only. My signature below acknowledges that I have been advised of, understand, and agree to follow district Policy 2035 – *Electronic Resources*, and accompanying Procedure P2035-1 – *Electronic Resources Procedures*. Violation of any of the conditions of use explained in the district's Electronic Resources policy or in these procedures could be cause for disciplinary action, including suspension or revocation of network and computer access privileges, and up to termination of employment.

Date:_____

Printed Name: _____

Signature: _____

School/Department: _____

Position: _____

(e.g., 4th grade teacher, education assistant, custodian, etc.)