Provo City School District

Policy Series 4000: Curriculum, Instruction, Assessment

4202 P2

Electronic Resources: Employees, Volunteers, Guest Users

The following procedures are written to support the Electronic Resources policy and to promote positive and effective digital citizenship among staff, interns, visitors and volunteers. 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-lasting impact on an individual's life and career. In this document, the terms "staff" and/or "employee" include interns, visitors, volunteers and district employees.

Network Services

As noted in Policy 4202, "network services" includes, but is not limited to, wired and wireless computers, devices and peripheral equipment, files and storage, e-mail and Internet content (blogs, Web sites, Web mail, groups, wikis, etc.). The district reserves the right to prioritize and restrict use of and access to the network.

"Network services" support education and research consistent with the mission of the district. Provo City School District owns the network provided throughout the district, along with all district-provided computers; the district therefore has the right to regulate usage thereof.

Communications on district computers and networks are public. Privacy should not be presumed and is not guaranteed, even for personal messages. Therefore, staff:

- Should not include personal addresses, pictures of self, phone numbers, location of school, social security numbers, employee ID numbers, and personal financial information in electronic communications.
- Should give notice immediately to a system administrator if they encounter materials that violate the rules of appropriate use, or if the messages or files sent to them contain threats, sexual references, or if they make them feel uncomfortable.
- Should not divulge their password to another person.

Use of the system must comply with state and federal law, network provider policies and licenses, and district policy. Use of the system for commercial solicitation is prohibited.

As a protection of the district's network and to manage technology demands within the restrictions of technology department staffing, the district reserves the right to deny internet access/network connectivity to personally-owned and non-district equipment. Connectivity of any personal electronic device is subject to district review and all guidelines in this document.

Acceptable network use includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational 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 educational research;
- The online publication of original educational material;
- Curriculum related materials and student work. (Sources outside the classroom or school must be cited appropriately.); and
- Accessing cloud resources such as e-mail, file shares, and other educational services.

Unacceptable network use includes but is not limited to:
- Personal gain, commercial solicitation and compensation of any kind;
- Liability or cost incurred by the district;
- Downloading, installation and use of games, audio files, video files or other applications (including shareware or freeware) except where prior approval from school principal, administrator, or the technology department has been given;
- Support or opposition for ballot measures, candidates and any other political activity;
- Using obscene, vulgar or inappropriate language;
- Hacking, cracking, vandalizing, disabling anti-virus software, the introduction of viruses, worms, malware, Trojan horses, time bombs, network scanning, etc. and making changes to hardware, software and monitoring tools;
- Unauthorized access to district servers, computers, electronic devices, networking equipment and information systems;
- Physically damaging computers, computer systems or computer networks;
- Cyber-bullying, hate mail, defamation, libel, harassment of any kind, discriminatory jokes/remarks/images;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- Using the equipment in any way that is inconsistent with individual school policies;
- Circumventing Internet or email filters to access non-CIPA compliant content. (CIPA – Children's Internet Protections Act);
- Possess, while at school or any school-related activity, any pornographic or sexually explicit material in any form on any device personal or District (Cloud storage services such as dropbox, copy, and sugarsync place digital copies of files on a your device);
- Violating copyright laws;
- Sharing passwords or granting access to a district network service by logging in for students, patrons, or employees;
- Using your password to authorize District information not directly necessary to accomplish current duties;
- Trespassing in others' folders, work or files (School officials may monitor folders, work, or files without permission or notice);
- Intentionally disrupting the system or wasting resources in any way (such as disk space, printing capacity or electronic intrusion);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the district network. Any such equipment may be confiscated.

The use of Network Services is a privilege, not a right. Inappropriate use will result in cancellation of those privileges and possibly other disciplinary or legal actions including criminal prosecution, suspension, expulsion or termination of employment.

Internet Safety

Personal Information and Inappropriate Content:

- Staff should not reveal student personal information, pictures/video of student or staff, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.
- Staff should not reveal personal information about another individual on any electronic medium.
- No student pictures, videos or names can be published on any class, school or district website unless the appropriate permission has been verified according to FERPA regulations.
- If district employees encounter dangerous or inappropriate information or messages, they should notify the appropriated school or district authority.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene or pornographic - 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 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters alone are not a solution.

Filtering Rules:

- Every user is responsible for his or her use of the network and Internet and must avoid objectionable sites;
- Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited. These attempts include, but are not limited to, the use of proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;
- Teachers and staff will provide appropriate adult supervision of Internet use.
- Staff 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.

Filters block the following categories:

- Adult Content, Sexually Explicit Content, Child Pornography, Pornography, Explicit Art, Obscene, Tasteless, and R Rated content.
- Security: Bad Reputation Domains, BotNet, Hacking, Malicious Code, Virus, Phishing, Spyware, Peer-to-Peer/Filesharing and Web-based Proxies/Anonymizers.

- Gambling
- Illegal/Questionable: Criminal Skills, Dubious/Unsavory, Hate and Discrimination,
- Illegal Drugs, School Cheating, Terrorist/Militant/Extremist
- Alcohol
- Tobacco
- All other CIPA compliant categories as required.

Exception Categories

- Education Material: Material under another category that has educational value (such as classic literature, sex education, etc.)

Copyright

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific 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 treated as copyrighted. Permission to publish any student work requires permission from the parent or guardian.

Network Security and Privacy

Passwords are the first level of security for any 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.

Every person is responsible for activity that occurs with their password. The following steps are required to safeguard network user accounts:

- Change passwords regularly;
- Do not use another'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 that 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 email use.

No user should presume any expectation of privacy when using the district's network, software or equipment. 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. During an investigation to determine whether this policy has been violated, the district reserves the right to submit a GRAMA request for a personal phone and personal account information if the phone/device service is paid for with district funds.

Disciplinary Action
All employees agree to all district policies at time of employment, and also yearly when they sign their contracts.

The use of district "network services" is a privilege, not a right. Inappropriate use will result in cancellation of those privileges and possibly other disciplinary actions including suspension or termination. Legal action, including civil and criminal prosecution, may also occur toward individuals who willfully cause damage to the district's network, equipment, and/or related services.

Approval date: December 11, 2012
Updated: November 24, 2014