Provo City School District

Policy Series 4000: Curriculum, Instruction, Assessment

Policy No. 4202

Electronic Resources

The Provo City School District Board of Education 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 students need to be proficient users of information, media and technology to succeed in a digital world.

Therefore, Provo City School District will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant, responsible and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology in schools just as individuals in workplaces and other real-life settings. The district's technology will enable educators and students to communicate, learn, share, collaborate and create, think and solve problems, manage their work and take ownership of their lives.

To help ensure student safety and citizenship in online activities, all students will be educated about appropriate behavior, including possible consequences of interacting with other individuals on social networking websites and in chat rooms, and cyber-bullying awareness and response.

Provo City School District provides Network Services to its students and employees. "Network Services" includes all computer hardware, network and Internet services and associated software. The District firmly believes that the valuable information and interaction available on the internet far outweigh the risks of users obtaining material that is not consistent with the educational goals of the district. Access to Network Services will be provided to students and staff who are expected to act in a considerate and responsible manner.

Provo City School District reserves the right at its discretion to access or monitor (with or without notice) use of any computer system connected to the district network. The reasons may include investigating or resolving network or communications problems, preventing system misuse, and ensuring compliance with legal and regulatory requests, and enforcing Provo City School District's acceptable use standards.

Staff and student disciplinary action may be taken if Provo City School District learns of inappropriate use of computing systems or networks.

The board directs the superintendent to create strong electronic educational systems that support innovative teaching and learning, provide appropriate staff development opportunities and develop procedures to support this policy.

Legal Reference:

Utah State Code 2510-2522	Electronic Communication Privacy Act
Adopted by Board of Education:	June 12, 2012
Revised:	December 11, 2012

Provo City School District

Policy Series 4000: Curriculum, Instruction, Assessment

4202 P1

Electronic Resources

Introduction

These procedures are written to support the Electronic Resources Policy and to promote positive and effective digital citizenship among students, 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.

"Opt-Out"

With technology growing in its relevance and usage in district classrooms, student will be using technology as a normal part of the learning process in schools. Therefore, it is assumed in this policy/procedure that students will have appropriate access to technology as part of or as a supplement to the education provided by the district. In the past, Provo School District has asked parents for permission to use technology with their students as an "opt-in" approach. The district now gives parents a choice to "opt-out," meaning that they may request that their child/children be restricted from accessing electronic resources at school. Please see 4202 F-1.

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 the use of and access to the network.

Using the definition of Network Services requires use of the district network, computers and all other district owned/provided Network Services to support education and research and be 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 should be assumed to be public in nature. As such, privacy should not be presumed and is not guaranteed, even for personal messages. Therefore, users:

- Should not include personal addresses, pictures of self, phone numbers, location of school, and personal financial information in electronic communications.
- Should give notice immediately to a parent, teacher or 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 never agree to get together with someone they meet "online" without first getting permission from their parent or guardian.
- 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.

Provo City School District maintains technology protection measures to monitor, track, and filter the use of Network Services, including Internet and Intranet, and reserves the right to suspend or revoke privileges and take disciplinary action for unacceptable use of the district network and property.

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 by district students and staff 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 with parental permission;
- 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 by district students and staff 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);
- 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);**
- **Violating copyright laws;**
- **Using another person's password;**
- **Trespassing in others' folders, work or files (School officials may monitor student or staff 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
Internet Safety Training is to be provided to minors by their school and will address:

- Appropriate online behavior
- Cyber bullying awareness and response
- Social networking sites
- Chat rooms

Personal Information and Inappropriate Content:

- Students and 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.
- Students and 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 students encounter dangerous or inappropriate information or messages, they should notify the appropriated school 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 are not a solution in themselves. 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 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**.**

Internet and Internet Filtering:
The Internet allows unprecedented opportunities for access to information for students and staff. The District maintains a fast connection to the Internet that is constantly monitored for utilization and efficiency, and is periodically upgraded to meet the growing needs of the district.

The district uses an advanced filtering solution that affords students and educators protection against objectionable Internet material.-There is also increased record keeping available to track Internet activities to individual computers. Provisions exist for requesting additional sites to be filtered or sites to be unblocked.

Filtering rules currently in effect block the following categories:

- Adult 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 unless the student is at least 18 years old.

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.

The following procedures are designed 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 e-mail use.

No student or staff user should presume 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.

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. All employees agree to all district policies at time of employment, and also yearly when they sign their contracts. Violation of any of the conditions of use explained in the-electronic resources

policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school for students, administrative disciplinary action for staff, or revocation of network and computer access privileges for students or staff.

Legal References

Utah Code 76-10-1235 Accessing Pornographic or Indecent Material on School Property

Approval date: December 11, 2012