Adoption Date: January 17, 1996
Revised: June 6, 2012

INSTRUCTION ELECTRONIC RESOURCES

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 than face-to-face interactions.

Network
The district network includes wired and wireless computers 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 control the use of, and access to, the network.

Use of the district's network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students and staff includes:
- Creation of files, projects, videos, web pages, podcasts and the like using network resources in support of educational outcomes;
- Participation in blogs, wikis, discussion forums, as well as the creation of content for podcasts, e-mail and web pages that support educational outcomes;
- The online publication of original educational material, curriculum related materials, and student work. Sources outside the classroom or school must be cited appropriately and in accordance with copyright laws;
- Staff use of the network for incidental personal use is not considered private and is carried out in accordance with all district policies and guidelines;
- Connection of personal devices to the district's guest wireless network for filtered Internet access. *Connection of any personal electronic device to the district network is subject to all guidelines in this document.*

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 without permission or approval from the district's IT Dept.;
- Support or opposition for ballot measures, candidates and any other political activity;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, or changes to hardware, software, and computer monitoring tools;
- Unauthorized access to other district computers, networks and information systems;

- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture, use of weapons/contraband…);
- Accessing, uploading, downloading, storage and/or distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated.

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 its 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.

Filtering and Monitoring

Filtering software is used to block or filter access to Internet content that is obscene and inappropriate for educational use, including all child pornography in accordance with the Children's Internet Protection Act (CIPA). As part of the general filtering policies enforced by the district's chosen software, other objectionable material may 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, https, 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 computers;
- 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.

INSTRUCTION ELECTRONIC RESOURCES

Network Security and Privacy
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.

These 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;
- 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.

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 message 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 nightly.

INSTRUCTION ELECTRONIC RESOURCES

Electronic Communications – Staff Guidelines:

Recognizing the challenges new forms of electronic communication and interaction introduce, the District provides the following guidelines for employees:

As representatives of the Deer Park School District, employee use of **Social Networking** sites in dealing with the District's constituents is governed by the following:

1. Employees may NOT utilize social networking services to conduct school business, conduct school-related communications with students or parents, or conduct school-related communications with other faculty and staff members (i.e. - Facebook, Twitter, Google+). All online class, club, or team management should be conducted via the District's approved web-based communication tools (dpsdmail.org or deerparkpages.com) unless otherwise approved by the Superintendent or Director of Technology.

2. Employees may NOT initiate or accept "friend," "follower," "circle," or "hangout" requests (or similar) from current students.

3. Employees must remain cognizant that the uneven power dynamics in a school environment – in which adults have both explicit and implied authority over students – continues to shape those relationships after the end of the school day, year, and even after graduation or separation from the district. Employees must act in a manner that always respects and never exploits the power inherent in these relationships.

4. Employees should consider carefully the dynamics of establishing Social Networking connections with current, former or prospective parents, and the line between personal and professional communication, in doing so. The lines between public and private, personal and professional are easily blurred in the digital world. As an employee of the Deer Park School District, you are connected to colleagues, students, parents and the greater school community. If you identify yourself as an employee of the Deer Park School District, you should ensure that online content associated with you is consistent with your professional obligations. *Employees are reminded that Social Networking sites are not an acceptable communication tool for conducting or discussing school business.*

As representatives of Deer Park School District, employee use of a **web-log ("blog") or wiki sites** in dealing with the District's constituents is governed by the following:

1. Employees may not utilize *personal* blog sites, wikis, or websites to conduct school business, conduct school-related communications with students or parents, or conduct school-related communications with other faculty and staff members. All official online class, club, or team management should be conducted via the school's approved web-based communication tools (dpsdmail.org or deerparkpages.com) unless otherwise approved by the Superintendent or Director of Technology.

2. Material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful or embarrassing to another person or organization is prohibited. Employees using the District's blogging or website platforms are expected to moderate comments and content.

INSTRUCTION ELECTRONIC RESOURCES

As representatives of Deer Park School District, employee use of **personal communications devices** (whether via voice or text message) in dealing with students in the District is governed by the following:

1. Communications between employees and students will primarily be direct, either oral or written, and *should be always pertinent to the student's educational experience*. When communicating electronically with students for educational purposes, staff members should use district provided devices, accounts and forms of communication (i.e. – computers, phones, telephone numbers, e-mail addresses, and district-provided publishing tools). If the use of district-provided devices and/or accounts is unavailable, staff members communicating electronically with students must do so in accordance with number two below.

2. Personal devices used for voice or text communication should only be used when necessary as it relates to a district-sponsored class or activity and only when district provided tools are not available or applicable. **Staff members are required to include an administrator in any text communications with students and should always inform an administrator/supervisor when the need arises to call a student's personal mobile number.** Staff members receiving text messages or calls from students should either forward the messages to their supervisor or report the communication directly.

3. The district prohibits staff members from communicating with students electronically for reasons other than educational purposes. This policy does not limit electronic communication of staff members who might be related to students or have contact with students outside the school environment through personal friendships, neighborhood or community activities, or participation in civic, religious or other organizations. *These contacts may justify deviation from some of the standards set in the policy, but under no circumstances will a personal relationship justify electronic communications with a current student that could be deemed as unprofessional, inappropriate, illegal, or criminal.*

Consequences for Violation of Policy

It is the responsibility of all users to follow all Deer Park School District policies and procedures as well as State and Federal statutes and laws. The consequences for violating the district's AUP include, but are not limited to, one or more of the following:

- suspension of computer access
- revocation of computer access
- disciplinary action up to and including expulsion/dismissal
- referral to law enforcement agency and/or Office of Professional Practices for further investigation, and/or
- revocation of a certified staff member's license(s) subject to review by the Office of Professional Practices

01/17/96, 07/14/00, 08/23/10, 06/06/12