Use the Internet with Care

Grand Coulee Dam School District promotes a safe, secure, reliable and technology-enriched learning environment for its staff and students through the use of technology to monitor Internet and other external traffic. This technology monitors, filters and captures Internet use, including e-mail, instant messaging, chat sessions, Internet web browsing and file sharing looking for specific types of content and flagging items that are not in compliance with the district's policies and procedures.

Among other things, the system promotes a safe, secure and productive environment by:

- improving staff and student safety by facilitating the investigation of threatening e-mail received by students or staff
- ensuring compliance with state and federal law by monitoring staff or student compliance with district and the State of Washington's K-20 Acceptable Use Policies
- improving the learning and working processes by notifying the appropriate personnel of students or staff who use their computer for non-education related activities
- helping protect private information of students and staff as required by law
- improving staff and student productivity by helping everyone focus on the educational mission and learning objectives of the district
- managing the network bandwidth needs to assure availability and performance in support of the districts educational mission

Here are a few reminders to everyone of the district's Internet Acceptable Use Policy that governs use of district computing and network resources.

Grand Coulee Dam School District's mission, strategic plan and board policies – not to mention state and federal law – mandate that its resources be used in direct support of the education of the students. Key elements of the policy include the following unacceptable behaviors or activities:

- Accessing any information that does not have educational or training value, or interferes with professional responsibilities or the educational process.
- Using any district computing or network resource for illegal, inappropriate, or obscene purposes. Examples: browsing pornography web sites, sending harassing e-mail, gambling, forwarding jokes or non-educational related information.
- Intentionally disrupting, degrading or harming the computing or network infrastructure. Examples: flooding the network with unauthorized traffic, deletion or corruption of system files, willful introduction of computer viruses or worms.
- Using the district's computing resources for personal, commercial or political gain or fraud. Examples: use of eBay to buy or sell non-district related items or run a home business from a district laptop, political lobbying
- Theft of data, equipment, or intellectual property. Example: printing and removing the benefits records of an employee without proper authorization, downloading unlicensed music, games or software.
- Gaining or attempting to gain unauthorized access of others' files or vandalism of the data of another user. Examples: purposeful deletion of another user's data on a shared drive, accessing systems or data without authorization or approval.
- Forgery of e-mail messages, use of an account owned by another user, or posting unauthorized or inappropriate messages. Example: unauthorized use of broadcast capability or email system to send non work-related messages to all users in a school or group.
- Possession of any data that might be considered a violation of these rules in paper, magnetic (disk), or any other form Examples: user IDs and passwords collected using a key-logger and stored on disk, thumb drive or sent via email, possession of hacker tools or information specific to the intrusion of the district network.

• Unauthorized access of information, acts of software piracy, hacking, and/or tampering with hardware and software. Examples: downloading or installation of games or software that the user does not have a valid license for, modifications or disabling of standard district PC system settings.

Use the Internet with Care

• Attempting to defeat or bypass the district's internet filter, security protocols or authorization. Example: using a proxy website to bypass the content filter to access a blocked website.

Frequently asked questions

Q: Can I install computer games on my district laptop?

A: No, unless they are a bona fide part of the curriculum for a class you are teaching.

Q: Can I check my bank balance from my PC at work?

A: Infrequently. Incidental or infrequent use for this type of purpose of a district PC during a scheduled break or time that does not interfere with your professional responsibilities is allowed.

Q: I buy and sell items on eBay. Is it OK for me to check the status of my auctions throughout the day so I don't miss out on an important bid?

A: No. Incidental or infrequent use of eBay during a break could be allowed, but using the network for any type of personal financial gain (e.g. the sale of items) or spending lots of time on eBay or other non-work related web sites is not allowed.

Q: Can I download and install software from the Internet onto my PC?

A: It depends. To ensure that any software loaded on district PCs conforms to licensing requirements, is free of viruses and Spyware, is compatible with the district's computing infrastructure and consistent with the district's educational priorities.

Q: Can I use my district laptop at home using my personal wireless network?

A: Yes, as long as you don't make any configuration changes to the laptop that causes it to not work on the district network. However, keep in mind that all Internet Acceptable Use policy rules apply no matter where you are using the laptop.

Q: During my off hours can I use my district PC or laptop to manage my personal checking account or use it to operate a nondistrict business or organization?

A: No.

Q: Are personal e-mail, instant messages or web browsing activities private?

A: No. There should be no expectation of privacy when using district computing or network resources. With the exception of specific information protected by law (e.g. covered by HIPAA or FERPA) all records, e-mail, web browsing activities (including exact images of what was viewed), chat sessions, files and documents are subject to the public records disclosure laws of the State of Washington.

Q. Could I be disciplined or fired for violating the district's Internet Acceptable Use Policy.
A: Yes.