Policy No. 2320
Instruction

ACCEPTABLE USE – COMPUTER EQUIPMENT

The purpose of this policy is to outline the acceptable use of computer equipment at WSD. These rules are in place to protect the employee and Washington School for the Deaf. Inappropriate use exposes WSD to risks including virus attacks, compromise of network systems and services, and legal issues.

Washington School for the Deaf (WSD) is committed to protecting its employees, partners and the agency from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of WSD. These systems are to be used for business and educational purposes in serving the interests of the agency, and of our clients and students in the course of normal operations.

Effective security is a team effort involving the participation and support of every WSD employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

This policy applies to employees, students, contractors, consultants, temporaries, volunteers and other workers at WSD, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by WSD.

General Use and Ownership

- There is no expectation of privacy of electronic mail; facsimile transmissions; NXI or voice mail stored as an electronic record; or information accessed, downloaded, stored or created on agency owned equipment. An electronic record is reproducible and is therefore not private. Such records may be subject to disclosure under the public disclosure law, or may be disclosed for audit or legitimate state operational or management purposes. While WSD network administration desires to provide a reasonable level of privacy, users should be aware that the data created on agency systems remains the property of WSD. Because of the need to protect WSD network, management cannot guarantee the confidentiality of information stored on any network device belonging or connected to the WSD network.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. WSD is responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems.

In the absence of such policies, employees should be guided by agency policies and practice regarding personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

- For security and network maintenance purposes, authorized individuals within WSD may monitor equipment, systems and network traffic, or examine records or files at any time, per the WSD Computer Workstation Security Policy.
- WSD reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by agency confidentiality guidelines, details of which can be found in Human Resources policies. Employees should take all necessary steps to prevent unauthorized access to this information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Use encryption of information in compliance with DIS Acceptable Encryption Use policy.
- Postings by employees from a WSD email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of WSD, unless posting is in the course of business duties.
- All hosts used by the employee that are connected to the WSD Internet/Intranet/Extranet, whether owned by the employee or WSD, shall be continually executing approved virus-scanning software with a current virus database.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- Filtering services are in use on all computers with access to the Internet. This will block or filter access to visual depictions that are obscene, including pornography; offensive or otherwise inappropriate images; sites that conflict with the mission of WSD.
- WSD staff will, to the best of their ability, monitor students' use of the Internet on the WSD network, and will take reasonable measures to prevent student access to inappropriate material on the Internet and World Wide Web, and restrict students' access to materials harmful to vulnerable populations.

Unacceptable Use

- **System and Network Activities**
- **Email and Communications Activities**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of WSD authorized to engage in any activity that is illegal under local, state, federal or international law or which is prohibited by applicable professional standards of conduct while utilizing WSD-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by WSD.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which WSD or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a WSD computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any WSD account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited without prior approval from the System Administrator.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, WSD employees or students to parties outside WSD.
- Downloading, storing, viewing or accessing pornography or obscene material is strictly prohibited by any individual on the WSD network or any agency owned equipment.
- Political or religious advocacy conflicting with Public Disclosure Commission (PDC) regulations is prohibited. Staff is responsible to contact the superintendent prior to use of the network if unclear of PDC regulations.

Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, NXI or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within WSD's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by WSD or connected via WSD's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Spam	Unauthorized and/or unsolicited electronic mass mailings.
DIS	Department of Information Services
WSD	Washington School for the Deaf
FTP	File Transfer Protocol
NXI	Nextalk – TTY phone access for the deaf through Internet Protocol (IP)

Ref: Chapter 42.52 RCW

Adoption Date: 12/09/04