NOLS
NORTH OLYMPIC
LIBRARY
SYSTEM

Policy HR 8.11
Computer Security Awareness and Acceptable Use

Adopted by the Library Board of Trustees: 04/26/2012
Revised: 01/24/2013

1. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at NOLS and is intended to protect the employees and NOLS. Inappropriate use exposes NOLS to risks including malware attacks, compromise of network systems, services and data, and legal issues. This policy applies to employees, contractors, consultants, temporary employees, and all other workers at NOLS, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by NOLS.

NOLS is committed to protecting all employees, partners and the Library from illegal or damaging actions by individuals, either knowingly or unknowingly. Computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and any other access to digital resources are the property of NOLS. These systems are to be used for purposes serving the interests of the Library, its partners and its customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every NOLS 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.

2. General Use and Ownership

a. While NOLS administration desires to provide a reasonable level of privacy, users should be aware that the data they create on Library systems remain the property of NOLS. Employees should not store personal information on Library-owned devices. NOLS cannot guarantee the confidentiality of employees' personal information stored on any network device belonging to NOLS.

b. Employees are responsible for exercising good judgment regarding the reasonableness of "personal use". NOLS administration and/or individual departments are responsible for creating guidelines concerning personal use of NOLS hardware, software and systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor.

c. For security and network maintenance purposes, authorized individuals within NOLS may monitor equipment and audit networks and systems at any time.

3. Security and Proprietary Information

a. The information contained on NOLS systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: patron information, personnel records, employee information and employee lists. Employees should take all necessary steps to prevent unauthorized access to confidential information.

b. Library staff will not accept identifying information from library users beyond what is required to create library user accounts.

c. Authorized users are responsible for the security of their passwords and accounts. Users must keep passwords secure; system and user level passwords should be changed every 90 days. Users may not share accounts, other than those accounts that are specifically designated for sharing to explicitly authorized users.

d. All PCs, laptops and workstations that are not physically secure or consistently monitored must be secured with a password-protected screensaver with the automatic activation feature set at 3 minutes or less.

e. Only Library staff, and explicitly authorized contractors, consultants, temporary employees and volunteers are allowed to log on to Library staff computers.

f. Library staff must secure their workstations by logging off or locking the desktop when the workstation will be unattended or unmonitored for longer than 3 minutes.

g. Because information contained on portable computers is especially vulnerable, special care must be exercised. Laptops must be protected in accordance with IT Department security standards.

h. All hosts used by the employee, which are connected to the NOLS Internet/Intranet/Extranet, whether owned by the employee or NOLS, shall be continually executing approved virus-scanning software with a current virus database, and shall have a personal firewall correctly configured and turned on.

i. Library staff must follow recommended IT Department security procedures and use extreme caution when accessing Internet resources and when opening e-mail attachments, which may contain viruses, malware or other hazardous code.

j. Only NOLS email accounts may be accessed on Library staff computers, unless personal email access is specifically authorized by the Library Director. Employees' personal email accounts may be accessed on the Library's public access computers.

k. Postings by employees from a NOLS email address to mailing lists or newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of NOLS, unless posting expresses an official NOLS policy or position.

4. Unacceptable Use

Under no circumstances is an employee of NOLS authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing NOLS-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.

5. Specifically Prohibited System and Network Activities

a. 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 NOLS.

b. Aside from legal "fair use", 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 NOLS or the end user does not have an active license.

c. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

d. Revealing account passwords to others or allowing use of NOLS accounts by others. This includes family and other household members.

e. Using a NOLS computing asset to actively engage in procuring or transmitting material that is in violation of applicable sexual harassment or hostile workplace laws.

f. 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.

g. Circumventing user authentication or compromising security of any host, network or account.

Email and Communications Activities

a. Sending unsolicited email messages, including advertising material to individuals who did not specifically request such material (email spam).

b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

c. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

d. Unauthorized use, or forging, of email header information.

e. Representing NOLS in public communications without authorization.

6. Enforcement

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

7. Administration

The Library Director has responsibility for administering this policy.