STND-5010-02: Technology and Equipment Use Standards
Origination: 05-10-2024
Effective: 07-09-2024
Reviewed: 07-09-2024
Last Updated: 06-06-2024

Technology and Equipment Use Standards

All technology users at Northern Pennsylvania Regional College ("NPRC" or "the College") agree to the following:

1. **TECHNOLOGY ACCESS –** The Information Technology Department is responsible for managing technology access within NPRC. This includes:

1.1 Providing network user accounts by adding, modifying, and deleting user access;

1.2 Overseeing training, policies, procedures, information security, resource use, and other administrative controls;

1.3 Ensuring protective guidelines that apply to data and technology access, use within the College, disclosure outside the College, electronic distribution, and/or disposal/destruction;

1.4 Ensuring information resource facilities will be physically secured by measures appropriate to their critical importance;

1.5 Determining security vulnerabilities and establish controls to detect and respond to threats to facilities and physical resources;

1.6 Providing the appropriate level of protection necessary to ensure integrity and confidentiality of critically sensitive data handled outside of secure areas;

1.7 Ensuring physical equipment will be secured and protected from physical and environmental damage;

1.8 Providing support for the instructional, research, and administrative activities for NRPC computing, telecommunications, and networking resources at the College;

1.9 Monitoring use and limiting, restricting, or extending access to electronic resources; and

1.10 Developing procedures to protect information resources from accidental, unauthorized, or malicious access, disclosure, modification, or destruction.

2. **TECHNOLOGY USE**

2.1 Information resources are designated for authorized purposes. The College has a right and a duty to review questionable employee activity. This must not include any unauthorized uses and must not interfere with the legitimate business of the College.

2.2 All information assets must be accounted for and be assigned Users. Users of information resources must be identified, and their responsibilities defined and documented.

2.3 Users are expected to conduct their activities within the restrictions and overall policies of NPRC, and federal, state, and local laws.

2.3.1 Agreement to abide by this standard is a condition of acceptance to use the College's electronic resources. Violators are subject to suspension of computer privileges and possible referral to the appropriate judicial or disciplinary process.

2.4 The following uses of Information Resources of the College are unacceptable:

2.4.1 Non-College-related political or charitable activities;

2.4.2 Commercial uses including, but not limited to, the promotion of "for profit" and/or privately-owned businesses or sale of private property;

2.4.3 Abuse, defamation, promoting harassment, or illegally discriminating on the basis of race, gender, national origin, age, marital status, religion, or disability;

2.4.4 Fraud or distributing any unlawful message(s);

2.4.5 Excessive use for frivolous, non-productive, and/or non-College-related purposes including, but not limited to, entering chat rooms and using social media; and

2.4.6 Other unauthorized acts or actions not in accordance with College policies or in the best interests of NPRC.

2.5 College Information Resources must be protected to ensure the College's ability to meet its educational goals. Therefore, the following actions are prohibited:

2.5.1 Theft, damage, or destruction of computing facilities, programs, or data;

2.5.2 Access or use of computing facilities, programs, or data that are not authorized to the User's account;

2.5.3 Sharing usernames, passwords, pin numbers, or any other Security related procedures; files or accounts with other individuals including, but not limited to, employees or students;

2.5.4 Inhibiting or disrupting the operability of computer systems, telecommunications facilities, networks, or other electronic resources; and

2.5.5 Intentionally introducing viruses, Trojan horses, worms, or similar potentially damaging or harmful programs onto any College systems or networks.

2.6 Users must not download, attach, change, distribute, or install any software or inappropriate files, including streaming content, for non-business functions (i.e., downloading MP3 files and/or broadcast audio or video files).

3. USER PRIVACY

3.1 Users should have no expectation of privacy of information stored on or sent through College-owned Information Resources, except as required by state or federal law. For example, the College may be required to provide information stored in its information technology resources to someone other than the User because of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. §67.101 et seq.).

3.2 Information stored by the College may also be viewed by technical staff working to resolve technical issues.

3.3 NPRC reserves the right to filter Internet site availability, and to monitor and review employee use as required for legal, audit, or legitimate authorized College operational or management purposes.

4. COPYRIGHTS, INFORMATION SHARING, CONFIDENTIAL INFORMATION

4.1 Users are responsible for their own awareness of the rights of copyright owners. Refer to NPRC-5025 Copyright for more information.

4.2 Users shall not share their User account information, including, but not limited to, the account's name, logon, password, or files for any reason.

5. Users are required to comply with legal protection granted to programs and data by copyright and license. No unauthorized software will be installed on College systems without the permission of the Information Technology Department.

5.1 Users must not send or share confidential information for unauthorized purposes.

5.2 Users must not attach or use devices on the College network that are not approved for use by the Department of Information Technology, Safety, and Facilities.

5.3 Users must not redirect confidential or privileged College data to a non-College owned computing device without proper authorization.

5.4 Users must not use unauthorized peer-to-peer networking or peer-to-peer file sharing.

5.5 Users must be accountable for securing his or her computer, and for any actions that can be identified to have originated from it.

5.6 Confidential, private, personally identifiable information (PII), Federal Tax Information (FTI), or other sensitive data (i.e., credit card numbers, calling card numbers, logon passwords, health information, or other protected information), must be encrypted or dissociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet.

6. VIRUS PROTECTION AND USER RESPONSIBILITIES

6.1 Virus protection software is included on all College computing devices.

6.1.1 The virus protection software will periodically scan the User's computer; and

6.1.2 Virus Protection and Security updates are automated and monitored by the Department of Information Technology, Safety, and Facilities.

6.2 NPRC is not responsible for any computer or electronic viruses that may be transferred to or from data storage medium.

6.2.1 Users must use their best effort to assure that the equipment is not damaged or rendered inoperable by any such electronic virus while in user's possession.

6.3 Users must not intentionally introduce a virus into a College-provided computer or withhold information necessary for effective virus control procedures.

6.4 To protect the College from hacker attacks, confidentiality breaches, viruses and other Malware associated with the use of email accounts, users must:

6.4.1 Select strong Passwords with at least eight characters (including at least one capital and lower-case letter, symbol and number) without using personal information (e.g. birthdays);

6.4.2 Keep Passwords secret by remembering them instead of writing them down or use a secure password database (e.g. Lastpass); and

6.4.3 Change Passwords at a minimum of every six months.

6.5 Users must never attempt to disable, defeat, or circumvent any security firewall, proxies, web filtering programs, or other security controls.

7. EMAIL AND USER RESPONSIBILITIES

7.1 All Users are assigned a College email account. The NPRC email system is considered an official means of communication, and all Users are responsible for information exchanged via their NPRC account.

7.2 Users are responsible for the maintenance of their assigned account including, but not limited to deleting unwanted messages and attachments.

7.3 Email can easily be forwarded to non-college accounts by the User; however, the User is responsible for the receipt of all information, including attachments, forwarded to another account.

7.4 Users are expected to check their NPRC email accounts on a frequent and consistent basis.

7.5 Use of assigned College email accounts should be primarily for NPRC-related purposes.

7.6 All Official electronic communication between NPRC Users shall occur using college-assigned email accounts.

7.7 Users must never execute programs or open e-mail attachments that have not been requested or come from an unknown source.

7.7.1 Check email and names of unknown senders to ensure legitimacy before opening or acting upon emails received.

7.7.2 If in doubt and lacking assurance from the sender, users should contact the Information Technology Helpdesk for assistance.

7.7.3 Avoid opening attachments and clicking links when content is not adequately explained (e.g. “Check this out! It’s amazing”).

7.7.4 Be suspicious of Clickbait titles.

7.7.5 Report all suspicious emails to the Information Technology Helpdesk

7.8 All users are encouraged to use an email signature that represents themselves and the College professionally.

7.9 Employee users are to use the supplied approved email signature. The template for the approved signature may be obtained from Hellbender Hub in the Marketing section.

7.10 College-assigned email accounts may not be used to:

7.10.1 Sign up for illegal, unreliable, disreputable, or suspect websites and services;

7.10.2 Send unauthorized marketing content or solicitation emails;

7.10.3 Register for a competitor's services unless authorized;

7.10.4 Send insulting or discriminatory messages and content; or

7.10.5 Intentionally Spam other people's emails, including their coworkers.

7.11 Users may use their College-assigned email account for all College-related purposes without limitations, including, but not limited to

7.11.1 Communicating with current or prospective students or partners;

7.11.2 Logging in to purchased software licensed by the College; and

7.11.3 Sharing their email addresses with attendees at conferences, career fairs, and other events.

7.12 Users may use their College email for personal reasons, including but not limited to

7.12.1 Registering for classes or meetings; and

7.12.2 Sending emails to friends and family provided the user refrains from generating spam or disclosing confidential information.

8. CARE OF NPRC OWNED TECHNOLOGY

8.1 Equipment must be kept in a laptop protective bag or case when not in office.

8.2 The protective bag or case containing the Equipment should be handled gently and never thrown or tossed around.

8.3 Care must be taken to keep any food, beverages, or liquids from spilling onto the Equipment.

8.4 Users will make no attempt to clean or repair the Equipment unless prior permission has been received from the Department of Information Technology, Safety, and Facilities.

8.5 One user account with specific privileges and capabilities shall be assigned to each laptop. The user agrees to make no attempts to change or allow others to change the privileges and capabilities of the assigned user account.

8.6 Users shall make no attempt to add, delete, access, or modify other user accounts on NPRC equipment.

8.7 Installation of peer-to-peer file-sharing programs is prohibited. File-sharing through use of audio and/or video file applications, such as iTunes or similar programs, is prohibited.

8.8 Users may not install or use any software other than software owned or approved by the Information Technology Department.

8.8.1 User agrees not to make any unauthorized use of or modifications of such software.

9. SECURITY INCIDENT RESPONSE

9.1 Users must follow PROC-5010-01 Reporting a Security Incident to report any observation of a successful or attempted data breach or security or privacy violation.

9.2 FORM-5010-01 Security Incident Form will be used to make the above report.

10. PHYSICAL EQUIPMENT USE AND STORAGE

10.1 Employees must guard against access to files and take precautions to protect technology devices when away from the workstation. This includes but is not limited to the following:

10.1.1 Logging off the computer;

10.1.2 Locking the computer; and

10.1.3 Locking the file cabinets, drawers, and office doors.

11. EXCEPTIONS TO STANDARDS

11.1 Standard Exceptions may be considered when there is justifiable business case(s), resources are sufficient to implement and maintain the alternate configuration, and all NPRC policies and procedures are followed and upheld.

11.2 To request a Standards Exception, users will submit FORM-5010-03: Standards Exception Request to their supervisor in accordance with PROC-5010-03: Standards Exception Request.

12. USER VIOLATION

12.1 Users found to be in violation of these standards or NPRC-5010 Information Security may be subject to disciplinary action including, but not limited to, suspension of access to technology resources and/or any action defined in NPRC-3235: Behavioral Code of Conduct for Students and NPRC-2110: Employee Code of Conduct.

13. USER ACKNOWLEDGEMENT

13.1 All Users must acknowledge receipt of the Technology & Equipment Use Standards and the Information Security Standards by completing FORM-5010-04: Technology and Equipment Acceptable Use.

14. REVIEW STATEMENT

14.1 Standards are reviewed as needed or when the related policy is reviewed in accordance with CLDR-1310: Policy Review Schedule.

15. APPROVAL

______________________________ ____________________________________ __________

Name Title Date

Revision Notes: Standards in Origination